THE FUTURE OF SOVEREIGNTY IN CYBERSPACE: UNDERSTANDING THE CHALLENGES OF INTERNATIONAL CYBERSECURITY

16TH - 18TH JULY 2012, SINGAPORE

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

GLOBAL FUTURES FORUM
CREATING NETWORKING POSSIBILITIES

NATIONAL SECURITY COORDINATION SECRETARIAT

THE FUTURE OF SOVEREIGNTY IN CYBERSPACE: UNDERSTANDING THE CHALLENGES OF INTERNATIONAL CYBERSECURITY

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)

16TH-18TH JULY 2012
MARINA MANDARIN HOTEL
SINGAPORE

CONTENTS PAGE

Rapporteurs: Sulastri Osman, Nadica Pavlovska, Valerie Teo, Jennifer Yang Hui, Yeap Suyin and Senol Yilmaz
Edited by: Jennifer Yang Hui and Damien D. Cheong

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 rule. Accordingly, beyond the points expressed in the prepared papers, no attributions have been included in this conference report.

EXECUTIVE SUMMARY

The Workshop on "The Future of Sovereignty in Cyberspace: Developing a Global Architecture for Cybersecurity" was held in Singapore at the Marina Mandarin Hotel from 16 to 18 July 2012. The Workshop addressed the theme of developing a global governance architecture for cybersecurity. It concluded that a global approach involving the public and private sectors was required to address the borderless security threats enabled by cyberspace.

The workshop began with a plenary speech entitled "Reconciling Westphalia and Cyberspace" by Eneken Tikk. She argued that with the increasing diversity of the concept of cyberspace it was imperative for nations and organisations to cooperate to resolve the numerous issues related to securing cyberspace.

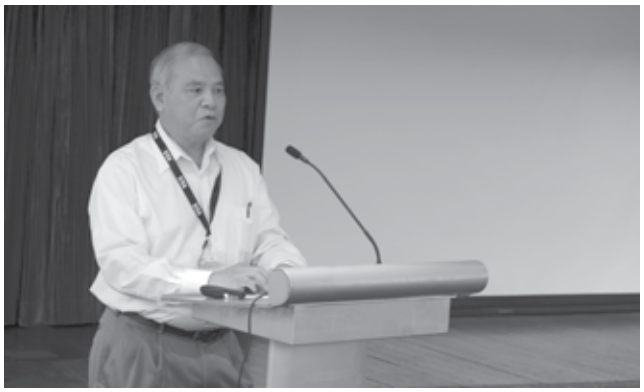
The first part of the nine-panel Workshop discussed cyberspace as a potential realm of conflict through the lenses of sovereignty, state responsibility, and international humanitarian law. The first panel outlined the rules of the road in administering the global architecture for cybersecurity. The proposed United Nations (UN) code of conduct and dimensions of active defence were explored. The second panel analysed the legal limitations and obligations in cybersecurity. The applicability of the laws of armed conflict and legal issues in attributing cyberattacks to a state were discussed. The third panel examined potential futures of cyberconflict related to the military dimension.

In the second part, the Workshop examined proposed models for internet governance and technical standards. In the fourth panel, speakers shared their organisational experiences in enhancing global cybersecurity readiness. The fifth panel highlighted the role of international standards and their implications on the technology marketplace. The sixth panel looked at the role of governance models to shape the best possible cyberfutures.

Finally, the Workshop explored the emerging role of non-state actors in the international system. The seventh panel examined the interaction between technology and politics as well as contemporary social and economic lives. The eighth panel discussed the role of the private sector in the global architecture for cybersecurity. The final panel considered how international organisations might incorporate cybersecurity norms in promoting economic and social development as well as to promote the freedom of information.

A Roundtable was dedicated to discussing the future of sovereignty in cyberspace over a 5-year and 20-year period. The session debated the future strength of sovereignty, raised possible research agendas with regard to cybersecurity, and discussed the future role of cyberspace in delivering international humanitarian objectives as well as the intersection between cyberspace and politics given the dynamics of contemporary international geopolitics.

WELCOME REMARKS BY THE ORGANISERS



Cung Vu from the National Maritime Intelligence-Integration Office (NMIO) and Global Futures Forum (GFF) of the US Department of State, welcomed speakers and participants to the Workshop on Cybersecurity held in Singapore at the Marina Mandarin Hotel from 16 to 18 July 2012. The Workshop was jointly organised by the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS) and the GFF, with the support of the National Security Coordination Secretariat (NSCS) in the Prime Minister's Office (PMO).

Vu said that this Workshop was the third in a series of Workshops on Cybersecurity organised by the GFF, which examined different themes. The inaugural Workshop in 2009 discussed "Towards a Secure and Resilient Cyberspace". Topics raised related to cybercrimes included terrorist attacks, financial fraud and dissemination of extremist propaganda throughout cyberspace. Additionally, the Workshop looked for ways to develop resilience and security in cyberspace. The second Workshop in 2011 discussed the geostrategic implications of cyberspace. It explored the dynamics of cyberspace in critical national and international issues such as economy, policy and legislation. It also looked at potential threats and explored policy options to address them from an international perspective.

This year, the Workshop theme was "The Future of Sovereignty in Cyberspace: Understanding the Challenges of International Cybersecurity". It aimed to address questions such as: (a) what an effective international cybersecurity treaty entailed; (b) how international organisations could foster cybersecurity norms; (c) the responsibility of the state towards non-state actors; and (d) the possible areas of mutual legal assistance in a global architecture for cybersecurity.

The Workshop was extended from two to three days this year because of a generally positive response. There were approximately 120 participants (including the speakers) from 16 different countries present, promising a robust exchange of ideas.

Kumar Ramakrishna, Head of CENS, welcomed the participants on behalf of Ambassador Barry Desker (Dean, RSIS) and the NSCS. He expressed his pleasure at the repeated collaboration with the GFF noting that the Workshop was the fifth time that CENS had collaborated with GFF. It was also the fourth time that he had worked with Cung Vu, who coordinates the GFF Communities of Interest on Emerging and Disruptive Technologies.

Ramakrishna told the audience that the Workshop would contemplate the future of sovereignty in cyberspace over the next three days. He noted that the world was experiencing rapid technological advances in the cybersphere. The need for clearer rules for all cyberspace stakeholders such as the government, civil society and private sector had become clearer than ever. To illustrate the growing discussion on cybersecurity, Ramakrishna alluded to a Straits Times article published two days before by Kenneth Rogoff entitled: "Cyber Threat: It's Folly to Just Shrug It Off". In the article, Rogoff suggested that it was important not to take cyberthreats lightly. He noted that the challenges of preserving international cybersecurity are extremely complex and thus, more time, expertise and resources were needed to cope with rapidly mutating cyberthreats.

Ramakrishna outlined the theme of this year's Workshop that ponders how we should move from the current Hobbesian state of affairs to one where everything was premised on a more stable and resilient global cyber architecture based on Westphalian norms. He cited Hedley Bull, a British scholar of international relations, who once asked whether it would be possible for international cyber societies based on widely accepted norms to evolve as the international society of states had done in the past 300 years. Posing this question to the audience, Ramakrishna added that this was the central idea that guided the presentations and breakout group discussions.

Ramakrishna also thanked both international and local speakers and participants of the Workshop. He encouraged the participants to be actively involved in the discussions and breakout group sessions, which were designed to generate deeper discussions and provide unique networking opportunities. He emphasised that one of the strengths of the GFF Workshops was the networking opportunities, and invited participants to exchange views and contacts freely during the Workshop.

Ramakrishna concluded by highlighting that the Workshop adhered to a variation of the Chatham House rule whereby all presentations would be on–record, but discussions were strictly off-the-record and non-attributable.

RECONCILING WESTPHALIA AND CYBERSPACE

In her Plenary Speech, **Eneken Tikk** observed that the concept of cyberspace had evolved significantly over time. She noted that different nations conceptualised cyberspace differently in light of national objectives. There were, therefore, varying lexicons when nations converged to discuss the issue of cybersecurity and cyberspace-related policy.

Tracing some of the historical milestones of international definitions and conceptualisations of cyberspace from 1969 to the present, Tikk said that in the beginning, the option to optimise some of the computer resources were not in the area of security. Being fundamentally an academic project, it was aimed at developing ways to interconnect computers. The internet was, at first, not viewed as a national security concern. For some time, cyberspace was a controlled environment, with known users and predictable sets of transactions. Network activities were also controlled fairly easily. This meant that legal concerns with regard to using computers were primarily focused on physical damages of the machines rather than virtual damage. Tikk also noted that early legal developments centred on allowing non-insiders to use the internet and making the system easier to use for non-insiders.

The notion that cyberspace was increasingly becoming a security threat was proposed in the 21st century. In 2001, the Cybercrime Convention was established. From 2007 onwards, the series of cyberattacks in Estonia, Georgia as well as the more recent Stuxnet incident, exemplified issues that were foreseeable since the late 1990s.

Tikk acknowledged that sovereignty in cyberspace faced a number of sometimes competing, but cumulative concerns that needed to be addressed. She showed the audience the architecture which currently existed, and the ways to resolve the aforementioned concerns. She also discussed the role of international organisations in resolving cyberspace-related issues as states were often unable to resolve such issues on their own. She noted that the private sector was an important player, but a difficult one to accommodate in the context of national security interests, especially when considering the significant amount of resources required for producing a comprehensive level of cybersecurity. Additionally, she said that users had also initiated regulations of their own. Tikk observed, however, that none of the existing legal provisions developed over the years had foreseen what the world was currently facing in terms of the constantly evolving cyberthreats. Nevertheless, this did not mean that such legal provisions were irrelevant.

Tikk concluded her speech by saying that she saw the issue not simply as one of Westphalia and cyberspace, but the complexity of the heritage that surrounds cyberspace. She acknowledged the existing work of international organisations in trying to address cybersecurity concerns, and believed that the full potential of such international organisations had not been truly explored yet.

Cybersecurity, for Tikk, could not be addressed simply by a single notion, because infrastructure, protocols and content were currently subject to different regulatory and governance regimes. Many varied interests and responsibilities were involved. No one organisation or actor was mandated or capable of resolving the whole puzzle. She believed that there was a need to compartmentalise the big issue of cybersecurity into smaller parts so that it would be easier to resolve the issues and interdependencies through discussions. At this juncture, Tikk opined that actors with the legal ability were not using their mandate and capabilities effectively.

Discussion

The following points were made during the discussion. On whether a global or hierarchical approach was more feasible in dealing with the issue of cybersecurity, most nations agreed that there was a need for state responsibility for cybersecurity. There were also many things that a country needed to do at the local level before even considering moving the issue to the international regulatory level. Only when these issues were resolved could there be international discussions.

A missing component was technological expertise and the role of the technologist in establishing a Westphalian order of governing cyberspace. While the input of the technologist was certainly needed, there was no set rule for specialist inputs: For example, input from the policymaker was necessary in explaining the concept of the Westphalian order to the people; the military was required to explain the consequences of cybersecurity measures; and lawyers were needed to explain the legality of cybersecurity measures as well as define the often confusing legal interpretations. There was a need to consider the applicability of existing cyber-specific laws. There was no need to further regulate cyberspace, but to apply existing laws.

Cyberspace was likened to a battleground where things were constantly evolving. Were policymakers and users of the cyberspace constantly being overtaken by people and events? What about the fluidity of the global architecture of cyberspace? While the architecture was fluid, the notion that cyberspace was a battleground and that users were losing the battle was rejected. The problem was not that laws were not keeping up with developments, but that users were trying to be too technology-specific in their responses.

Finally, noting that much of sovereignty was built around geography, in cyberspace, geography was more fluid. How could geography be incorporated into the discussion? While geography would not make sense in every context, this did not mean that it was not relevant. Geography should be used from a geographical perspective, not in a virtual perspective. One area where the concept of geography might pose a problem when discussing cyberspace was the issue of attribution.

PANEL 1: RULES OF THE ROAD

The Proposed UN Code of Conduct in the Realm of Cybersecurity: Balancing Contradictory Goals

Alan Chong examined the proposed UN code of conduct for the internet through the discourse of national sovereignty within the wider context of globalisation. He noted the difficulties of managing the global information infrastructure and underscored the challenges of cybersecurity: a term defined as the means and policies of securing cyberspace from disruption and activities that resembled armed aggression in the offline world.

Chong said debates about the future of the internet and concerns over control in cyberspace paralleled the debates of the New World Information and Communication Order (NWICO) of the 1950s to 70s. The debates had then helped shed light on the multidimensional meaning of sovereignty as well as relations between the state and society. Such issues continued to be relevant in the internet era, as was evident by the International Code of Conduct for Information Security that was drafted in 2011 by four UN members: China, Russia, Tajikistan and Uzbekistan.

Chong highlighted a number of salient points the document alluded to. For one, the four governments had linked national security with international stability and infrastructural security; second, they also considered sovereignty in internet policy integral to international cooperation; third, information security capacity building and the closing of the digital divide were important to work towards; and finally, supply chain security needed to be established considering the extent to which the internet had been integrated into many aspects of governance.

From the document, Chong also teased out three sets of perspectives regarding sovereignties in cyberspace: (a) territorial sovereignty; (b) ideological normative sovereignty; and (c) intellectual sovereignty. Territorial sovereignty, Chong explained, was what nation states claimed in order to rule over and decide on the laws of the (physical) land, but its adoption in cyberspace was problematic. Legal spaces would require some degree of territorialising, yet territories in cyberspace could not be easily demarcated. Further, territorial sovereignty would require a government to practise political socialisation – or the more contentiously termed 'propaganda' – for the sake of stability, which was another thorny subject in the porous cyberspace.

Ideological normative sovereignty was another dimension that featured in debates on internet governance because notions of nationalism and other communitarian interests were often extended into cyberspace. Such issues had considerable emotive sway, and in an online environment, the ones which were more controversial in nature were difficult to control, and could pose possible security concerns. Chong provided the example of unverified rumours regarding inter-religious violence. He also noted that racist sentiments were hard to police online.

Intellectual sovereignty was another much debated and contested dimension. Fears, especially in non-Western and developing economies, of creative dominance by private corporations who owned a large portion of information communications technology, persisted. The logic of the private marketplace often clashed with the idea of national sovereignty. Copyright laws were also argued to be the means of structural control by the West. Additionally, many battles over international reputation would continue to be wrought out in cyberspace.

Chong concluded by arguing that there was a need to balance national security considerations when attempting to develop norms in cyberspace as national security remained a *de facto* framework for understanding policymaking. Accounting for the territorial aspect of policymaking was important too, considering the contentious issues that an individual like Wikileaks' Julian Assange could give rise to. Finally, the private sector needed to be consulted on issues of internet governance although the solutions would not always prove equitable.

Technical, Legal and Policy Dimensions of Active Defence

Herbert Lin compared and contrasted passive defence and active defence in cyberspace, and examined their implications for conduct regulations in the online realm. Passive defence, which included firewalls and antivirus programmes, was defined by the US Department of Defense (DoD) as measures taken to reduce the probability and minimise the effects of damage caused by hostile actions without the intention of taking the initiative. Passive defence was largely actions operated within the domain of organisational custody where the organisation had accountability over the boundaries. Such actions were generally reactive to hostile intrusions, and there was a clear understanding of what 'hostile' denoted; antivirus software, for example, could recognise a previously identified malware and subsequently eradicate it.

Active defence, on the other hand, could mean any actions taken outside the organisational domain. In practice, active defence was essentially anything that was not passive defence. The DoD defined active defence in cyberspace as synchronised, real-time capability to discover, detect, analyse and mitigate threats and vulnerabilities that was built on traditional approaches of defending DoD networks and systems. It operated at network speed using sensors, software and intelligence to detect and stop malicious activity before it can cause damage.

Active defence could be undertaken either within or outside the organisational domain. When dealing with an adversarial system within the organisational domain, one could practically: (a) distract and delay intruders by setting up a system specifically designed to attract adversarial intrusions, i.e., honeypots; (b) deceive intruders by feeding them corrupted files and misinformation; (c) reroute or drop traffic from intruders; (d) allow interactions only with white-listed parties, software and computers that had authenticated themselves; or (e) dynamically reconfigure defences and networks. Lin pointed out that the policy significance and legal implications of active defence within organisational domains were fairly limited.

However, the policy and legal issues associated with active defence outside the organisational domain could be considerable. Lin listed out the different kinds of active defence responses to an adversarial system using a two-by-two matrix, which was based on two important characteristics: intrusiveness and damage. An active defence could be considered: (a) non-intrusive and non-damaging, i.e. deep packet inspection of malware in flight and deletion of packets or beaconing from adversary systems; (b) intrusive but non-damaging, i.e. intelligence gathering; (c) non-intrusive but damaging, i.e. "spike" bad software, remotely disable pirated/stolen software or information, or mirror traffic, or neutralise the incoming threat (if unknown); and (d) intrusive and damaging, i.e. retaliate and/or pre-empt adversary attack capabilities and neutralise incoming threats.

The acts of defence that were non-intrusive or non-damaging could be referred to as non-offensive defence. They would still raise policy issues, however, because they were less controversial, thresholds were lower and attribution errors, if any, were less significant. Nevertheless, such operations could still be considered illegal; an intelligence-gathering operation, for instance, could sometimes be mistaken for an attack. The acts of defence that were considered intrusive and damaging on the other hand, could be defined as offensive defence where issues of threshold and attribution were of great significance along with the question of promptness and scale of response(s).

To conclude, Lin raised a number of important policy issues. He asked to what extent there should be coordination among different actors in cyberdefence, and what were to be the roles of the military, law enforcement and intelligence communities. He also asked if changes had to be made to existing legal regimes to facilitate active defence and if active defence should not be limited to DoD assets only but extended to private entities as well.

Discussion

The following points were made during discussion.

Would active defence change in a situation of cyber conflict? An ongoing fight would change it completely because in an all-out war, nobody was going to pay much attention to the nuances in policy implications. However, in a case where the adversary was known, the kinds of policy issues brought up regarding active defence would still matter when acting against other (unknown) opportunistic adversaries that might be trying to intrude.

What was the dividing line between offensive information warfare and active defence and how could one identify the differences between the two? The difference between offensive information warfare and active defence was that the goals of active defence were typically much more limited, i.e. to get the adversary to stop his/her disruptive activity and perhaps dissuade future actions; it did not presume an ongoing conflict. That said, the technologies and/or capabilities used in either circumstances could be exactly the same.

Who decided on the level of securitisation of assets and the threshold? Those questions had no good answers at this point as the appropriate rules of engagement were still being fleshed out.

What could governments reasonably allow the private sector to do by way of active defence? It was doubted any desirable outcomes were possible if governments were to regulate what the private sector could do in that regard; however, it was not certain if letting the private sector have free reign to do whatever they wanted was the way to go either. There were certainly initiatives in principle that the private sector could do because governments did not always have the necessary resources at hand.

PANEL 2: LEGAL LIMITATIONS AND OBLIGATIONS

The Applicability of the Laws of Armed Conflict to Cybersecurity

In her presentation, **Heather Harrison Dinnis** discussed when the laws of armed conflict would apply to cyberoperations. She began by discussing cybersecurity as a new war-fighting domain, and pointed out that many of the world's militaries had already recognised this in both official and non-official capacities. Most notably, the United States military had recognised cybersecurity as the fifth domain in which it operated. Nonetheless, when discussing the military potential as well as threat of cyberspace, it was important to bear in mind that the idea of cyberspace, as a new and unique war-fighting domain, was a strategic concept and not a legal one.

That being said, she pointed out that the laws of armed conflict (LOAC) did apply to the new technological developments because many of the laws were drafted as general principles. The Geneva Convention, the Martens Clause of the Hague regulation of 1948, and the other instruments governing the conduct of hostility, were drafted at a time when computers did not exist and thus, they did not specifically refer to cyberwar. Nevertheless, these laws were flexible enough to deal with, and accommodate new developments in technology, so they were not restricted to the means or method employed. She emphasised that while cyberspace provided new challenges for interpretation of the LOAC and there was room for further intervention in this field. There was no doubt that the principles of the LOAC did apply to cyberoperations being conducted during hostilities.

In addition, she explained that in order to have a situation of armed conflict, one needed to have some minimum threshold level, which was difficult to identify since there were different thresholds depending on whether one was dealing with International Armed Conflict (IAC) or Non-International Armed Conflict (NIAC). IAC was defined as the resort to armed conflict between states. Therefore, the problem with cyberattacks was that it is difficult to ascertain if the attacks could be attributed to a state or not, as illustrated in the Russia - Georgia case.

On the other hand, NIAC involved protracted armed violence between governments and organised armed groups, which meant that a certain level of intensity of violence, protraction, level of organisation must exist, and the conflict must cause certain amount of damage before the NIAC could apply. These criteria were difficult to establish with regard to cyberattacks as the damage was intangible, the violence was not physically present, the organisation was also not present, and it can be perpetrated by individuals or by groups.

Clearly the IAC threshold was much easier to meet than the NIAC threshold, but the problem in cyberattacks was that one could not be sure of the source of the attacks, whether it was a state or an internationally organised group or individuals, hence, one could not know which criteria it should meet.

Harrison Dinnis then proceeded to describe the meaning of an "attack" and the participants in the attack. In the definition of an attack, she focused on the Schmitt/ Dörmann (ICRC) debate where the only point of consensus was physical harm, which clearly constituted a reason for armed conflict. However, difficulty arose when the attack was intangible, when the attack did not cause 'real-world' harm, e.g. turning off a power grid, instead of destroying it. The debate centred over whether this constituted an armed attack or not. On one hand, Schmitt argued that attack meant physical destruction, violence, death, and injury whereas on the other hand, the ICRC view was that even if intangible, the attack could cause the same amount of harm as the tangible attack, and thus, should be regarded as an attack. However, in recent times, a compromise was reached with the concept of functionality. If the functionality of something was destroyed and it had to be repaired, this would constitute an attack.

Harrison Dinnis also talked about participants in conflict, and in particular, about combatant status and direct participation in hostilities. Combatant status was relevant because as a combatant, a person would possess combatant immunity, and if captured, they would be given the status of a "person of warfare". The discussion on direct participants in hostilities was relevant because non-combatants would be considered civilians, and civilians could also be regarded as direct participants if they were engaged in cyberattacks. Therefore, the rule of reciprocity meant that direct participants were also targetable, not only by cyberattacks but by traditional armed attacks as well.

In conclusion, she stated that other issues that needed to be discussed were: (a) perfidy and what it meant to behave treacherously in cyberspace; (b) arms control treaties and whether they work in cyberspace; and (c) neutrality and obligations of third states. Lastly, Harrison Dinnis questioned if there was a need to change the definitions of property, as property now applied to the virtual world, and needed protection as it does in the physical world.

Identifying the Attribution to a State: The Study of the "Influence" Factor

In her presentation, **Setsuko Aoki** focused on how to identify the responsible state in the event of a cyberattack. She began with listing the responses that a sovereign state could legally employ against various attacks under existing international law.

She then proceeded to discuss the laws applicable to the use of force in cyberspace: *jus ad bellum* and *jus in bello*. She clarified that the law of war governed how states justified their engagement in war *jus ad bellum*. In other words, they determined the conditions necessary when lawful military force was employed. When the state suffered damage from a cyberattack from another state in the absence of military force, it was difficult for the victim to pursue the matter in the international court of law. In both cyberattacks and kinetic attacks, an attack was judged by the application of *jus ad bellum* or international humanitarian law.

Aoki said that the question was how the attribution to the "State" was decided in the event of a breach of international law. This was very difficult to establish, and thus, it was necessary to develop certain legal criteria. While there was no international treaty, a UN general assembly resolution titled "Responsibility of States for Internationally Wrongful Acts" had been adopted in 2011 and could be applied in some cases.

Aoki pointed out that attribution of a cyberattack to a state would be evident if the attack was conducted by an organ of the state, regardless of whether that organ was part of the executive or legislative, local or central levels of the government. In this case, the state could be held responsible. In the second case - if an organ of a state was not part of the government but acted under the control of the government - it would be seen as a *de facto* organ of the state as in the 1986 Nicaragua case. In the third instance, when a person or a group of people was acting under the direction or control of the state, they would be deemed to be agents of the state. She clarified that while such groups acting in their own capacity may not be an actual state organ, their strong connection with the state would nevertheless render that state accountable.

In addition, Aoki spoke about situations where the state was under an obligation to prevent certain acts from occurring and as such, could be held accountable even though the attack could not be directly attributable to

the state. For example, in accordance with the 2007 ICJ Genocide Convention Case, it is the obligation of the State to prevent certain acts of non-nationals carried out even outside its territory, as this may be based on the "influence" exercised by that State.

Aoki concluded her presentation by arguing that adopting a Cyberspace Cybercrime Convention or protocol was not enough, as only one aspect of cybercrime was addressed. Secondly, judicial cooperation and extradition of criminals prevented many states from acceding to this Convention. Lastly, she suggested that soft law/rules (e.g. code of conduct, guidelines, etc.) were more desirable, less time-consuming, and easier to reach consensus on.

Discussion

The following points arose during the discussion.

On the definition of damage and destruction in relation to a "cyberattack" alluded to in their presentations, the speakers were asked to discuss if cyberspace created new kinds of destruction, damage and harm that had not been traditionally contemplated, and how that should be factored in the contemporary view of *jus in bello*. It was agreed that cyberspace had introduced a new level of issues, and that the main contention was whether the damage caused had to be tangible. In relation to this, the Schmitt/Dörmann (ICRC) debate agreed that the existence of physical damage was tantamount to an attack having taken place. However, the definition of an "intangible attack" was debatable. As for the functionality test, it should be considered as an attack if the functionality of something was destroyed. However, the functionality criteria introduced a level of subjectivity. Nevertheless, destruction beyond the physical might also count as "damage" in legal terms.

As for economic damage to a country, for example whether bankrupting the country through a cyberattack would also constitute "damage", it was stated that economic damage could not be justified as *jus ad bellum*. There was, however, some shift in positions among states that previously held that economic damage might not be regarded as actual damage. This was noticeable mainly among developed countries that have now acknowledged that they are economically vulnerable to cyberattacks. Nevertheless, current international law did not view economic damage as a reason for *jus ad bellum*.

As cyberwarfare was completely different from anything previously seen, it was argued the world would need a new set of laws because LOAC could not be applied to cyberwar. However, it was pointed out that although cyberspace has emerged as a new territory, the LOAC is much generalised and as such, the principle of distinction was still applicable to cyberspace as it did not distinguish the methods or means of warfare.

PANEL 3: POTENTIAL DOMAINS OF CONFLICT

Cyberpower: West to East or East to West?

Rex Hughes presented on the apparent shifts in global cyberpower. Cyberpower had links to economic power, which by extension, comprised both soft power and hard power. It was at the intersections of these points that both opportunities and challenges presented themselves. However, in order to fully understand the power dynamics in cyberspace, Hughes argued for a new theory of cyberpower; there was no theoretical framework or reliable method to measure cyberpower at present.

Drawing on American political scientist, Joseph Nye's work on geopolitics, Hughes argued that power shifts were occurring on two levels: it was making a transition from West to East, and diffusing from state to non-state actors. From the technologists' perspective, power was also shifting from the analogue to the digital and from the disconnected to the connected. While the core of cyberspace remained dominated by Western entities, principles and norms, the ascendency of China and other rising Asian powers had made it less Western-dominated. Hughes added that difficult economic times ahead and a troubled Eurozone would likely contribute to a net decline in Western geostrategic power and global cyber power. He saw Asia's so-called tiger economies as leading the way in cyberspace today. They had pursued strategies on growth that was focused on high-level technology manufacturing and electronics and/or making the transition to service-based economies largely anchored in financial services and other knowledge-based industries. These services increasingly depended on robust connectivity and access to cyberspace.

Hughes believed that China, Japan and India – "the three Asian lions" – could have deep impact on cyberpower. China, for one, was becoming an economic superpower. While it had made little original technological contributions to the global political economy of cyberspace, its indigenous technological research and development had become highly relevant. China had also not hesitated from exerting its power in cyberspace and the military leadership left little doubt that it would advance or defend Chinese national strategic interests in the cyber domain. Observers continued to watch future developments in China: whether it would continue to maintain its relatively closed political system and a rigid control over information against a fairly open cyberspace.

On the other hand, Japan's technological prowess was already internationally acclaimed. Iconic brands were linked to heavy industries like ship building, aircraft and robotics, and aerospace technologies, all with dual use for defence. Hughes saw that Japan could become a new influential player in either the commercial sector or the military domain. With Japan's recent re-entry into the global defence market, one could expect interesting future developments in new technologies and applications.

In the case of India, Hughes mentioned that its low-cost labour matched with good technology meant it had a robust presence in the service sector. India was also increasingly playing an important research-and-development role in many top US firms, and doing well in developing indigenous capabilities by way of its large conglomerates. While India might face challenges in building a sound intellectual property regime with its IT prowess and sound economy, it could intensify the cyber quotient of its defence systems. In today's battlefield, weapons systems were moving towards networked-centric interactivity and the ability to write complex soft codes would translate into real cyberpower.

In conclusion, Hughes reiterated that cyberpower was an important measure of global power and it would continue to grow in Asia. As countries become more technologically savvy and connected, their influence in cyberspace would expand at a similar rate. He added that their growth in terms of cyberpower, however, need not be a case of zero-sum for the West.

Potential Domains of Conflict: Protecting Critical Assets

Dagfinn Buset spoke on the challenges of protecting critical assets from a Norwegian perspective. Despite having a small population, Norway, like Singapore, was considered an important global economy with a strategic geographical position that allowed it access to vast natural resources. As Norway was the second largest exporter of gas in the EU and the world's sixth largest exporter of oil, ensuring the protection of its critical infrastructure and critical societal functions was an important matter of both national and global interests.

In Norway, critical infrastructures were defined as constructions and systems that were considered essential to the continuation of society's critical functions. The interconnectivity and interdependency of the country's critical infrastructures – all of which were underpinned by ICT – meant that cyber incidences could disrupt or destroy infrastructures in one section and create damaging effects in other sections, thereby crippling critical societal functions. A higher baseline of protective security measures in businesses and sectors responsible for the operation of critical infrastructures and the provision of critical societal functions was thus needed, leading the government to enhance the role of the Norwegian National Security Authority (NSM). The NSM helped implement and coordinate security standards, with cybersecurity forming an integral part of its agenda. The NSM also dealt with the challenges that constant advances in technology brought; Norway's decision to adopt a new technology that would make possible the remote controlling of electricity consumption, for instance, would greatly benefit the economy and the environment but would increase security vulnerabilities that straddled between the cyber domain and the physical world of power production and supply.

Besides having to balance innovation and economic interests on one hand and public security interests on the other, the NSM also needed to balance the interests of the public sector with the private sector as many of the country's critical infrastructures were privately owned and operated. Buset said building public-private partnerships based on dialogue and trust was therefore crucial. The Varslings system for Digital Infrastruktur (VDI), an early warning system for cyberthreats against critical infrastructures, was highlighted as a prime example of cooperation. Buset explained that all partners in the VDI-system were either owners of critical infrastructures or suppliers of critical societal functions from sectors such as banking and finance, energy, health, defence and telecommunications, and the NSM allowed them full control over the sensors in the warning system. Among other things, partners could get assistance on incidence handling, or receive information, alerts and warnings on other related incidences. While there were, at times, dilemmas to work through, such partnerships remained essential for security.

Based on statistics from the Norwegian Computer Emergency Response Team (NorCERT), the number of cyber incidences and serious data breaches increased in recent years, a trend Buset attributed to a general lack of risk awareness at all levels of society in an ever more complex threat environment. Sound risk management processes were thus important, and cybersecurity needed to be an integral part of existing risk management policies. That said, Buset also noted the need to be aware of the delicate relationship between technological possibility, regulation possibility, and political desirability. He cautioned that democratic values could be challenged by increased security measures that could infringe on civil rights and liberties. There had to be a balance between robustness and preparedness.

Buset concluded by mapping out the physical presence of more than 100 Computer Energy Response Teams (CERT) across Europe. As cyber incidences were hardly confined to one country, international cooperation was critical. Shared vulnerabilities required shared cooperation in cybersecurity.

Future Domains of Cyberconflict - from Japan's Perspective

Motohiro Tsuchiya started his presentation on the future domains of cyberconflict with reference to several recent incidents that affected Japan. He said that Japan was hit in March 2011 by an advanced persistent threat (APT) in the form of infected emails. Confidential data was later stolen from the Mitsubishi Heavy Industry, a company involved in military construction for the Japanese government. And in November 2011, email passwords of Diet members were lost. There were a number of other attacks that the Japanese government suspected were linked to China as well, but issues of attribution as well as national sovereignty made the prosecution of such cyber activities very difficult.

Tsuchiya moved on to discuss the network of undersea cables, which he argued had been greatly overlooked as a potential vulnerability. This was an important issue for Japan because it was highly dependent on undersea cables for much of its communication functions. The issue over public security had increasingly become a concern because more and more of such cables were run by private corporations, which meant that the government was gradually losing control over the protection of its critical infrastructure. The Asia Pacific Gateway (APG) cables that linked many countries in the region together, for example, were operated by a consortium of private companies.

The maintenance of the undersea cables, according to Tsuchiya, continues to be a public security issue. Many people were adversely affected when communications were cut off during the Taiwan earthquake in 2006 and the eastern Japan earthquake in 2011. Other than being at risk in times of natural disasters, the undersea cables remained easy targets as they were not buried under the seabed. Adversaries could cut off communications via the underground maintenance tunnels and the cable landing systems. Tsuchiya pointed out on the map of Japan that there were two areas in the country where most of the cables were concentrated; China, South Korea and Singapore similarly had such areas where cable points were concentrated. These areas could be attacked easily, and the cable landing stations and related facilities were the easiest targets. It was therefore important to ensure better security for such sites. However, considering the high costs to protect these sites, coordination with foreign operators and governments as well as cooperation with private corporations that operated the undersea cables was necessary. He concluded that securing undersea cables should therefore not be overlooked when discussing the security of the cyber domain.

Potential Domains of Conflict

In her presentation, **Eneken Tikk** discussed several issues she believed shaped the discussions that were taking place within the North Atlantic Treaty Organisation (NATO), the European Union (EU), the United Nations (UN) and the Organisation for Security and Cooperation in Europe (OSCE).

With regards to issues such as offensive and active defence capabilities in cyberspace, NATO was encumbered by political restrictions, particularly in light of the absence of real situations on which to base the discussions. Furthermore, with increasing diversity in individual national opinions regarding cybersecurity, finding consensus was problematic. Tikk believed that should there come a time for an operation, more issues would emerge regarding funding, capabilities, what could be done and which procedures to adopt. These were issues NATO had yet to figure out.

The EU had begun the processes of drafting a document on cybersecurity. Beyond practical discussions such as which institute should be in charge and whose agenda should lead the way, Tikk listed a number of contentious issues. Firstly, there were varying concepts of privacy. Also, the EU's views on personal data protection were also likely to differ with those of other nations when it came to security. She argued that such issues would ultimately have to be mitigated at the national level.

The UN had developed a number of initiatives in relation to cybersecurity. For example, the International Telecommunication Union (ITU), the UN's lead agency on ICTs, served as a prime example of how an international organisation extended its mandate to pursue a new course of action. It was a process that started with member nations choosing to take an issue to the international organisation and the latter accepting the issue and building up an agenda around it. The UN had committed to discussions on international information security from the perspective of disarmament, but a closer look would show that there had not been much discussions regarding thresholds of cyberattacks or what to do about it. Tikk said it was important to be able to recognise and draw on the strengths of the UN's various components as it would produce more benefits for the international community.

At the OSCE the discussions were shifting from debating norms in cyberspace to a more practical discussion on confidence-building measures (CBM). Many parallel CBM processes were taking place at the bilateral level; at the same time, the OSCE was also conducting much background work on the issue of cybersecurity for the UN. However, Tikk argued there was often no clear position. She said that the international reality could be largely characterised by an absence of strategic perspectives of countries. However, the situation was gradually changing, and while conversations on cyberspace were no longer just limited to Russia and the US, not every country had formed their positions yet.

In conclusion, Tikk said that the potential domain of conflict was not simply between perpetrators and victims, but between countries that were searching for cybersecurity solutions. At the national level, the issue of content was paramount and restrictions were based on the available infrastructure as allowed by the existing authority. Nations would also continue to debate over semi-public security measures like critical infrastructure protection; they would need to figure out the levels of security that would be needed and who would pay for it. On the international level, the challenge of language and lexicon remained; it was important to be able to come up with standard lexicons for everyone to understand one another when talking about international information security.

Discussion

The following points arose in the discussion.

It was asked whether there was an impetus for smaller NATO nations to pool their resources together to meet their cybersecurity needs in spite of massive defence cuts in Europe. It was stated that pooling resources was viable for many countries small or otherwise. A coalition of smaller NATO countries could come together to express their views on cybersecurity. However, this carried specific risks too, considering they would have to ensure they possessed the necessary capabilities – military, among others – should an operation be carried out.

It was noted that in the two World Wars, cable cutting was considered a legitimate act of war and/or pre-emptive attack. This supported the view of the importance of securing cable networks and concentration points. As for whether it would be better to build more cable landing points, diversify, and have allies co-host them instead of simply improving multilateralism, it was agreed that co-hosting cable landing systems was possible, and it was already in practice. The Asia-Pacific Gateway cables, for example, had Chinese, South Korean and Japanese stakeholders, which meant they had common interests in securing the cables.

On the conceptualisation of cyberpower, and how a nation could improve its relative standing in that regard, it was stated that cyberpower was essentially a combination of hard and soft power, and considering that so much of cyberspace was in the hands of the private sector, it was crucial to keep tabs on the economic dimension of it. At the same time, it was equally important to account for the military dimension. It was crucial to focus on the interaction between the two because it would be the point of strategic competition.

Considering governments had a finite amount of money to spend on critical infrastructure protection, was there an efficient way to spend it on solving existing problems in terms of risk management? It was pointed out that achieving total security was virtually impossible no matter how much money was spent. Instead, government spending could be optimised to achieve a targeted level of security. To that end, the Norwegian government would use its limited resources to raise risk awareness through programmes like information campaigns and forge partnerships with the business sector in order to encourage them to engage in protective security. It was also important to properly organise the various actors and stakeholders responsible for maintaining cybersecurity in the country, as such, there was a need for some sort of coordination entity that could help with this task.

PANEL 4: OVERSIGHT AND ADMINISTRATION

Securing Cyberspace:
A Public-Private Shared Challenge

In her presentation, **Ruth David** focused on public-private partnership in ensuring security in cyberspace. She first explained that there were two different perspectives regarding the public-private partnerships: One being generally more positive and open to this kind of partnership, and the other, more sceptical that the private sector could contribute to cybersecurity. She concluded that both perspectives had merit, and the challenge was to find the common ground for both perspectives.

Explaining why cybersecurity was a shared challenge, she emphasised that cyberspace was fundamental to the modern global economy, and cited examples of e-commerce and e-government to elucidate her point. In both examples, it was clear that the public needed private assistance in cybersecurity. If one focused solely on the narrow view of cybersecurity, that is, as national security, then it was evident that the national security apparatus relied on the resilient cyberinfrastructure provided by the private sector for its command, control and continuity. She further argued that cybersecurity was fundamental to cyberspace and also emphasised that cybersecurity was advancing in tandem with cyberspace.

David explained that there were various models of public-private partnerships. Some of them were based on contractual agreement between a public agency (federal, state or local) and a private sector entity, while others were cooperative ventures between the public and private sectors.

She listed a few examples of public-private partnerships in the field of health, transport and energy, and argued that some of the motivations for forging these partnerships were for the purpose of producing a global public good and leveraging the capital investment of private investment for private-public good, e.g. transportation. In the field of energy, for instance, the primary reason for forging partnerships was to leverage the innovation capacity of the private sector for shared benefit.

Subsequently, David discussed the complicating factors for private-public partnerships in cybersecurity. She pointed out that issues of property, both intellectual and in asset valuation, could cause complications for these partnerships. She also stressed that there was a lack of basic regulatory structure, and therefore, there was a need for a new approach. Lastly, she explained that the time spent on cyberdevelopment, incident response and threat indications were all vastly shorter than anything in other private-public partnerships.

In conclusion, David argued that when discussing public-private partnership, it was first important to talk about the notion of information sharing. This was an area in which the motivations were common both for the private and for the public domains. In regard to information sharing, she argued that areas where poor decisions may be induced by a lack of information or misapprehension of the risks should be complemented by the state's role in facilitating better individual decisions through information or gentle interventions, which would influence the perception of risk, rather than supplanting them.

Maintaining Operability and Resiliency
in the Administration of Global Architecture
for Cybersecurity

Zahri Yunos emphasised that the main purpose of his presentation would be to provide practicable solutions, and strategies to assist in achieving security and safety in the cybersphere.

He commenced by defining key areas of insecurities in cyberspace. The main features of cyberspace were: (a) anonymity; (b) absence of regulation (as no country ruled nor owned the internet); and (c) its borderless nature (because laws were confined within boundaries). Nevertheless, ICT had changed our lifestyle, which was evident by the way we did business, banking, e-governance, etc.

Yunos said that the risks in the form of cyberthreats were also changing. If there were large scale, widespread incidents such as viruses or worm outbreaks in the past, now there were specifically targeted tools such as a Yack, Botnet, Stuxnet, and Flame. In addition, whereas the motives of the cyberattacks were previously for fun, prestige or peer recognition, they were nowadays carried out for more malicious purposes such as economic gain, industrial espionage, and cyberterrorism.

He further noted that hostile activities such as Hacktivism were increasing in cyberspace. Examples which illustrate this were anonymous attacks against established organisations such as the Central Intelligence Agency, US Congress, MasterCard, Visa, Sony PlayStation network, Turkey and NATO websites. Apart from Hacktivism, attacks on critical sectors had also been taking place, such as the ones over specific operating systems that employed the Microsoft platform. An example for this would be Dug Flame, a malware which collected sensitive information for the purpose of espionage.

In order to maintain operability and resiliency in the administration of global architecture for cybersecurity, Yunos suggested the following areas of focus: (a) public-private partnership; (b) regional and global cybersecurity cooperation; and (c) development of a legal and policy framework. He argued that national capabilities were indispensable; however, they should also be strengthened by regional and global partnerships.

In conclusion, Yunos stressed that no single nation could work alone in the area of cybersecurity as cyberthreats were trans-border in nature. Therefore, governments needed to strengthen public-private partnerships, and the international community had to also strengthen global cooperation. Additionally, there was a need to manage the weakest link of cybersecurity education, and it was important to take more proactive and responsive approaches in dealing with cyberthreats.

Enhancing Global Cybersecurity Readiness: ITU-IMPACT Case Study

Datuk Mohd Noor Amin spoke about cybersecurity from the perspective of the International Multilateral Partnership Cyber Threats (IMPACT). He introduced the partnership as the cybersecurity executing arm of the UN's specialised agency – the International Telecommunication Union (ITU) – which brought together governments, academia and industry experts to enhance the global community's capabilities in dealing with cyberthreats.

In discussing partnerships in the field of cybersecurity, he began by giving an example of the success of the international community in dealing with the spread of infectious diseases such as Ebola and SARS. He noted that this was mainly because of the strong partnerships that were forged on a global level, not only among governments but also between governments and private entities. He pointed out that there were many parallels that could be drawn between the outbreak of infectious diseases and the spread of malicious ware or cyberthreats. In addition, he attributed the success of dealing with contagious diseases mainly to organisations such as World Health Organisation and CDC, which did a splendid job of bringing different stakeholders together, including pharmaceutical companies, to deal with the problem for the benefit of the global community.

Amin then explained IMPACT's work in the field of cybersecurity. He spoke about how IMPACT was forging public-private partnerships across different stakeholders in the field of cybersecurity and stated that partnerships between the private sector and academia were also important. He emphasised that the governments did not have all the answers, and the challenge was greater when multiple stakeholders were involved.

IMPACT, as a cybersecurity executing arm of the UN, was mainly tasked to translate ideas into action, and transform recommendations into concrete programmes. At the moment, there were around 144 members that had joined the ITU-IMPACT coalition, including both advanced and developing countries. Some of IMPACT's partners included Microsoft, Symantec, Karspersky. It also cooperated with academia such as the EC-Council. Amin also spoke about prospective collaboration with INTERPOL.

To conclude his presentation, Amin enumerated the tasks the IMPACT had been undertaking. He explained that such tasks varied from aggregating threat information from different sources by relying on partners, to establishing more active collaboration in the Electronically Secure Collaborative Application Platform for Experts (ESCAPE) platform. He described ESCAPE as a platform similar to that of Facebook, but open only to experts, where they could exchange information and knowledge on new cyberthreats. In addition, IMPACT provided training to over 900 cybersecurity professionals and practitioners, provided scholarships in the area of cybersecurity, and trained 50 law enforcement officers from five countries. Lastly, he mentioned that IMPACT also provided cyberdrill exercises such as the one conducted in Myanmar. IMPACT also organised the first Arab cyberdrill in Oman, which involved different participating countries.

Introduction to the INTERPOL Global Complex for Innovation

In his presentation, **Eugene Soh** discussed the progress of the development of the INTERPOL Global Complex of Innovation (IGCI), which was a new initiative currently in the process of implementation. IGCI was organised around the following five areas: (a) capacity building; (b) digital forensics; (c) information sharing; (d) operational and investigation support; and (e) partnership development. He further explained that the new INTERPOL Digital Crime Centre would focus on three core areas: (a) cybercrime investigative support; (b) research and innovation; and (c) cybersecurity. The main vision of the INTERPOL Digital Crime Centre was to make cyberspace more secure while maintaining its openness. This goal was to be achieved through networking, leveraging information, knowledge and experience and lastly, harmonising global efforts for cybersecurity. In line with the main points raised by some of the previous speakers, Soh stressed that the partnership building would also be essential for INTERPOL. He explained that in the current inclement economic condition, contributions were also at risk as several countries were facing economic difficulties. Therefore, INTERPOL had to find alternative sources of funding and expertise in order to continue to deliver effective services to the global police community.

Soh said that INTERPOL would provide support for cyberinvestigation upon request by any member state. Thus, the goal of IGCI would be to provide the indispensible tools and technology, and more importantly, increase the network of investigators through building trust. The next function of the INTERPOL Digital Crime Centre was research and innovation, which would evaluate new technologies. To this end, INTERPOL would collaborate with academia and private companies, and would examine new methods and techniques. Lastly, in terms of harmonisation, like the many actors in the field, the INTERPOL Digital Crime Centre would try to avoid duplication of efforts, and therefore look into what other actors, such as international organisations, private companies and academia were doing in this field.

Soh also spoke about the process of building the capabilities of the INTERPOL Digital Crime Centre. This basically included bilateral discussions, cyberenvironmental scanning, and listening processes. The Digital Crime Centre was expected to be fully operational by May 2014.

In closing, Soh said that the IGCS would not replace the General Secretariat of INTERPOL in Lyon but would enhance its work. The IGCS, through sufficient funding from the Singaporean government, would be constructed within 24 months, and the ICCS building in Singapore would be the latest addition to the INTERPOL community, which had offices in South America, Africa and also a liaison office in Bangkok, Thailand.

Discussion

Elaborating on the role of the international non-governmental organisations vis-à-vis the state in problem-solving, it was noted that many of the key players in the IT sector as well as the other sectors which relied heavily on global trading and commerce provided a new and useful perspective because they operated in multiple jurisdictions. This was a unique and valuable perspective for securing cyberspace. If individual governments or international government organisations impaired the ability of the private sector to operate seamlessly in cyberspace, they would, in turn, handicap the economy, which would expectedly be detrimental to all parties. It was a matter of understanding the perspectives that all parties provided and recognising that they do operate in a relatively seamless manner across national boundaries. Therefore, the key was to enable rather than impede such activities.

DINNER LECTURE

GEOPOLITICS 2.0: AN INDUSTRY PERSPECTIVE ON BALANCED RISK ANALYSIS

Andrew Cushman's presentation focused on the extent and consequences of government activities pertaining to cyberspace from an external industry perspective. There were a number of challenges in dealing with cyberspace: these involved the interactions of states, industries, citizens and civil society. They were all transformed by the internet and there was a need to redefine the interactions between these different constituents. Often highlighted were the political and military dimensions of challenges faced. Cushman was, however, of the view that there were other dimensions alongside politics and military which should be considered as well.

One of the key points brought up by Cushman was that the cost-benefit analyses often missed or undervalued certain variables. One example was the variables concerning long-term consequences, which were undervalued when taking short-term gains into account. There was a need to do better in considering collateral damages from state actions in cyberspace. There were also unintended consequences that unfolded over time and were undervalued when making decisions.

Cushman listed a number of key changes that had taken place in the global ecosystem. Primarily, the world changed from being at the stage of "internet adoption" to being "internet dependant", almost overnight. This meant having approximately 2 billion internet users, 5 billion devices and 10 trillion interconnected devices in the not-too-distant future. In mapping the security landscape in cyberspace, challenges included: (a) having to deal with many malicious actors that had similar techniques; (b) being in a shared integrated domain; (c) the speed at which attacks could occur; and (d) consequences being hard to predict.

The real challenge in managing risks was that there were only certain things that were known, while a lot still remained unknown. Along the way, there was a need to balance short-term needs and longer-term implications. Further, in contemplating actions in cyberspace, there appeared to be a trend whereby decision-makers were contemplating attacks in cyberspace in the same way as they would physical attacks. However, while attribution was easier in physical attacks, it was extremely difficult to detect in cyberattacks.

In conclusion, Cushman reiterated the fact that cost-benefit analyses should be improved by including analysts outside the usual domains to better reflect other costs. A more informed set of opinions could help deliver more robust decisions, and it was important, therefore, to explore other collateral damages. Finally, the internet today rested on a foundation that had developed organically. Attacks made against some of the foundational elements of the internet affected the integrity of these elements, which could result in unintended consequences.

Discussion

The following points emerged in the discussion.

Was there a clash of interests or culture between the public and private entities or a convergence of interests? It was noted that the point of convergence was in the dependence of both the public and private sectors on the internet. There was clearly a convergence of interests in making sure that a society dependent on the internet continued to function properly.

On the notion of sovereignty and a borderless cyberspace, it was posited that communications over the last twenty years had slipped out of the control of national governments. This happened overtime through organic means and nations were trying to re-exert control over communications. There was a new "norm" and things would not go back to the way they were. While aspects of geography would be layered on top of a global internet, it would not look like the way it did in the past.

PANEL 5: SETTING STANDARDS

The Role of International Standards and their Impact on the Technology Marketplace

Goh Seow Hiong's presentation focused on the necessity of standards, the issues surrounding standards, and the role of governments in setting standards and important considerations in doing so.

Goh began by stating that only 20 percent of the economic benefits of ICT were in its production and 80 percent in its use. Hence, governments that were concerned about security implications of procured products had to consider that national production might increase security. However, this might not necessarily make sense economically. At the same time, he emphasised that ICT technology impacted the economy by improving the firms' modes of production and transforming individuals' daily lives. Goh also emphasised that communication networks were the fourth essential infrastructure beside energy, water, and transport.

The reasons behind the necessity for standards were three-fold. Firstly, standards guaranteed interoperability so that different products from different manufacturers could work together. Secondly, standards were required in a situation where no single company could solve a technical problem by itself. Thirdly, there were manifold problems that could arise when there were no standards.

According to Goh, there were a number of challenges surrounding standards-setting in the IT sector. First, standardisation bodies were not very structured. Furthermore, because development in this sector was rapid, governments could lag behind, and sometimes government imposing standards could even hamper innovation. Often, the market chose a standard which was not the best standard in technological terms. For example, Video Home System (VHS) was technologically inferior to the Beta standard, but it still won the competition in the market.

Goh also explained the role of governments in standards development. Governments were both policymakers - in the sense that they tried to promote choice, innovation, and economic growth - and customers at the same time, procuring products based on needs and requirements. Goh opined that governments should ideally allow flexibility to encourage innovation and regulate only when public safety concerns were involved. It could also be prudent for governments to avoid developing local standards and use international standards to meet their requirements. This would allow domestic producers to market their products globally and leverage economies of scale, and would provide greater choice to consumers.

Development of Information Security Standards at the International Level

Chan Kin Chong talked about the development of information security standards at the international level and provided an overview of the related working groups.

Chan began by recalling that the Singapore IT standards committee was formed in 1999 with the intention of establishing a framework on standards. At the time, it was recognised that Singapore was merely adopting standards rather than designing standards according to its own needs. Its members were experts and representatives from the industry, government bodies, academia, and research institutes who worked on a voluntary basis. Presently five working groups are active: (a) Business Continuity/Disaster Recovery (BC/DR) Working Group; (b)

Cryptography Working Group; (c) Cloud Security Working Group; (d) Information Security Management Standards (ISMS) Working Group; and (e) National Authentication Framework (NAF) Working Group.

So far, five Singapore Security Standards were published: (a) SS 493: 2001: IT Security Standards Framework; (b) SS 501: 2003: PKI Security Standards – Framework Overview; (c) SS 507: 2008: Standard for Business Continuity/Disaster Recovery Service Providers; (d) TR 29: 2012: Technical Reference for National Authentication Framework – Authentication Operator Interface Messages; and (e) TR 31: 2012: Technical Reference for Security and Service Level Guidelines for the Usage of Public Cloud Computing Services.

Chan provided an overview on the International Organisation for Standardisation and the International Electrotechnical Commission. In particular, he talked about the subcommittee for security techniques which has five working groups: (a) Security Management; (b) Cryptography and Security Mechanisms; (c) Security Evaluation, Testing and Specification; (d) Security Controls and Services; and (e) Identity Management and Privacy Technologies. Chan also enumerated a number of international development projects by Security Management, Security Controls and Services, and Identity Management and Privacy Technologies working groups.

Finally, Chan provided an introduction to the Regional Asia Information Security Exchange (RAISE). RAISE was a forum initiated by Kang Meng Chow, the former Chairman of the Security & Privacy Standards Technical Committee in Singapore. It was now co-chaired by Kang Meng Chow and Koji Nakao from Japan.

Towards a Trusted Cloud

Aloysius Cheang, presented on Cloud Security Alliance's (CSA) five-pronged strategy to make cloud technology secure and trustworthy. Referring to Chan Kin Chong's presentation on standardisation, he opined that standardisation played an important role when a given technology or issue had matured and its boundaries and challenges were clear. In the case of emerging technologies such as Cloud, there did not seem to be a unified understanding of what it was. Therefore, efforts to establish standardisation before this technology could mature might pose significant problems to developers.

As the standardisation working groups of the ITU meet in Geneva, Chan argued that many smaller stakeholders could simply not afford to send their representatives due to financial limitations. He concluded that the standardisation agendas in this body were dominated by a few influential countries or companies. For this reason, CSA was founded in 2009. Presently, CSA has over 36,000 members, 200 corporate members, and about 20 affiliated members. Its main objective is to increase trust in Cloud technology.

One of the ways to achieve this goal would be a five-pronged strategy. Firstly, there were obvious needs for standards, and CSA represented its members in standard-developing organisations. The second component of the strategy was education. CSA worked on best practices for Cloud computing and conducted flagship research projects. A source of information was the CSA Wiki. CSA also offered training courses such as Cloud Security Knowledge. The course prepared the students to take the CSA Certificate of Cloud Security Knowledge (CCSK) examination. The third component of the strategy was building a security framework. The fourth component was assessment. In this context, CSA launched the CSA Security, Trust and Assurance Registry (STAR), which was a free and publicly-accessible registry that documents the security controls provided by various Cloud computing offerings. The fifth and final component of the strategy was the creation of Cloud for the future: a comprehensive Cloud security reference architecture would be built. A survey of Cloud providers' governance practices in the market, for example backup, encryption, and secure deletion was part of this effort. The insights of this survey are currently being translated into best practice recommendations.

Discussion

The panelists were asked what the sovereignty concerns were in the various standard-setting organisations, it was stated that at the International Telecommunication Union Telecommunication Standardisation Sector (ITU-T), some issues were very political; since members often represented their governments, they pushed for their national interest. However, at the International Organisation for Standardisation (ISO) level, representatives in the working groups were not supposed to pursue the interests of their countries. Members of working groups also contributed their expertise on subject matter as individuals, and a solution was developed through consensus. It was only at the plenary level that each national representative voted in accordance with his or her national interest.

PANEL 6: ALTERNATE GOVERNANCE MODELS FOR THE BEST CYBERFUTURES

Existing and Alternate Governance Models

In his presentation, **Jason Healey** listed several different cyberfutures and the different approaches to these future scenarios in terms of: (a) the balance between offence and defence; (b) adversaries; (c) violence and frequency of conflicts; and (d) the nature of conflict and military operations. Healey asserted that the future scenario would be status quo in terms of the kinds of conflict that we would face. He argued that we would face the same kinds of conflicts of crime, espionage, denial of service, and the same relationship between offence and defence because for the last 40 years offence had always been easier to conduct than defence.

While it was hoped that in the future, defence would become much stronger than offence, in that it would be far more difficult for attackers to do what they want, Healey surmised that this ideal was possible but difficult to achieve. He stated that "Cybergaddon", a situation where offence was far better than defence, was a more likely scenario for the future. However, Healey argued, the relationship between offence and defence could switch relatively quickly with a single disruptive technology. For example, the invention of machine guns shifted the dynamics of war between the Napoleanic and First World War eras quickly.

Healey also pointed out that balkanisation was another feature of cyberspace in the future. Balkanisation of the internet would take place as countries become more competent at defending their own borders as geography was introduced into cyberspace. The world would comprise a whole collection of national cyberspaces and as a result, domains of conflict would change. Healey believed that a full range of conflicts where offence and defence interacted would take place by 2030. For example, he foresaw cyberversions of the Battle of Britain, the 1918 Battle of San Miguel, Vietnam War and Pearl Harbour. Additionally he believed that there would be large-scale cybersupport to regular battles. However, as most conflicts had historically taken place over a long period of time, Healey thought that in the future, there would be a long-term war with combatants that repeatedly come back over a protracted period. Therefore, this much wider range of conflicts would require different kinds of cooperation involving not just countries, but corporations and civil society as well.

There were three traditional approaches to cyber problems: (a) technical; (b) criminal; and (c) warfare. They had all been useful but Healey believed that these would not lead to the future where defence trumps offence. He saw that new approaches, such as the protection of international public health, cleansing of the environment and challenge of existing goals, e.g. to have zero weapons, were required. As new mindsets and new norms were inherent in terms of the environmental model, more space for non-state actors would be created to take the world out of the security-privacy tension.

Private Sector-Led Governance

Building on his speech about the ways in which the internet was changing, **Andrew Cushman** analysed the on-going debate about Internet Governance (IG). Cushman noted that nations were now realising that there was a need to reassert sovereignty over the internet,

and explained what IG was and how it had worked. He delineated changes to IG that were still in progress and offered some proposals for IG.

Cushman identified three key dimensions of governance: (a) physical infrastructure; (b) the "code" or "logic" layer that did not necessarily have borders; and (c) the "content" layer, which was content and usage. In light of the expansion and diversification of the global online population, the shift from West to East and North to South in internet populations, two main groups, i.e. the Regional Internet Registry (RIR)/Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Engineering Task Force (IETF) were formed for IG. Standards were made from working group recommendations with open feedback periods and policies were made from open discussions and voting by the groups' key main group members. There was, however, little or no governance of social issues like privacy or human rights despite the fact that the internet was very much a bottom-up phenomenon. Discussions were largely about administrative and technical interoperability rather than usage, and there was no governance for privacy or content. The ITU treaty had more restrictive membership requirements and voting, including governments, telecom companies and academics. Areas covered by the treaty included traffic flows between telecom network operators, quality of international services, sufficiency of facilities, international routing, charging, accounting and billing between operators. Cushman opined that priorities should be given to health and safety and the avoidance of harm to networks and services.

Cushman laid out several proposals that would impact industry and customers and ultimately productivity: (a) internet traffic charging; (b) heavy telecom and internet regulation; and (c) rate setting. Cushman argued that the ITU had a role in internet architecture governance by taking over standard-setting and by expanding its scope of regulation to include data-processing. He argued that IG was important because policy impacted a broad range of topics, i.e. secure Border Gateway Protocol (BGP), Domain Name System Security Extensions (DNSSec) implementation, submarine cable resilience, etc. He laid out an IG Framework comprising interoperability (treaty style, technical, political and administrative interoperability) and usage (activity, grievance and enforcement) dimensions. In his conclusion, Cushman stressed that it was imperative to continue "multi-stakeholderism" as he saw it as a relatively easy way to achieve cyberspace balkanisation.

Balancing Freedom, Security and Sovereignty

Bill Woodcock focused his presentation on what countries could do to increase their cyberdefence posture. He argued that it was important for countries to know and control their borders, be self-reliant within their borders and to establish trust relationships with their peers.

Firstly, in cyberspace, a country's border was its perimeter of control, a complex set of circuits and devices with multiple kinds and layers of access within which countries have ultimate control of the circuits and devices. Woodcock argued that the first step to controlling the interior was to accurately know where the border of control lay. He stressed that it was important to have a redoubt, a minimum perimeter of absolute control beyond which the state could not be compressed, the core from which the state could recover. This required complete knowledge of the terrain. In cybersecurity, the adversary dwelled in remote, unknown areas of systems. Circuits, routers, and servers were specific and comprehensible devices, and knowledge of the terrain they defined must be direct and literal, not abstract and analogous as there were differences between models and reality.

Second, states must be self-reliant in: (a) building internet exchange points; (b) domain name resolution; and (c) domestic human and infrastructural capacity. Internet Exchange Points (IXPs) were the sources of internet bandwidth. The IXPs that carry the most traffic were in Tokyo, Hong Kong, Seoul, Osaka, Palo Alto, and Seattle. Asian countries were increasingly establishing their own

IXPs to decrease dependence on exchanges in other countries. Yet, there remained 105 countries that did not have domestic IXPs although there were 350 IXPs in the world, all of which were very successful, fast and cheap to build. Self-reliance in domain name resolution was also important because people's ability to find things on the internet depended on a hierarchy of domain name servers. In order to find and communicate with a server, there was first a need to connect with a root name server and a top-level domain (TLD) name server. Countries were increasingly moving to host their own root and TLD name servers to gain autonomy from international fibre. It was also important to build human and infrastructural capacity domestically. For example, law enforcement dependence upon foreign-owned carriers for intercept capabilities meant that information could be leaked internationally, and as a result, the agency would receive intercepted intelligence that was compromised.

Third, it was important to establish relationships of trust. CERTs were the hub of trust relationships. Woodcock stated that it was important to be aware of what other people were trying to do in the governance of cyberspace and to understand one's own interests. He noted that the idea of alliances that was well-understood in military and politics was not well-understood among IXPs. Countries could have the same kinds of relationships as in the real world but there had to be a quid pro quo, e.g. good law enforcement, and a CERT. Woodcock cited Brazil as an excellent example of forging IXP alliances, and noted that while the internet had grown over 115 percent in the last few years, state-centric governance resembled the ITU model more than the internet model where each state was monolithic and the number of states relatively static. He stressed that interactions between state-level governance and IG must occur with a keen eye to differences not only of scale, but of rate of change in scale.

Discussion

Asked whether the extent of conflict in cyberspace was based on deep balkanisation, it was pointed out that even if the world were completely balkanised, problems would still arise. It was stated that the issues were interconnected. Balkanisation was an illustration of the scenarios put forth in the presentation, but it was possibly the easiest scenario that would also fit with other ideas. It was insufficient to think about the ways to reach the ideal scenario of defence being stronger and better than offence, but defence-offence was just a short-hand depiction. In the end, nobody knew how cyberspace would develop in the future.

Another point made was the political implications of shareholders' stakes in internet companies. In Mauritius, the privatisation of telecoms, which happened when Mauritius' telecoms was sold to French telecoms, ended ISP monopoly and ended sovereignty. Mauritius telecoms were no longer an agency of the Mauritian government. Likewise, Scandinavian companies had now become pan-Scandinavian. In the internet world, that was a mark of success, which did not necessarily align with state or national interests. The internet was built by the private sector for its interests, and was therefore more of a hindrance than support to national governments in general.

Questioned how defence could be stronger than offence in the future when Stuxnet and other developments were still in the quiver, it was noted that while "Cybergaddon" was inevitable, it was possible to lower the cost of control for the same level of governance and security in the hope of possibly getting to a more utopian future. Intrusions tended to be more politicised and therefore, undermined trust between countries. It was important to recognise that every attack differentiates the security "haves" from the security "have-nots", and that some people get more hardened, more defensive and stronger with attacks.

Asked whether they thought cyberweapons would be used on a large scale, one optimistic view was that they would not be used on a large scale by Western nations. When the US and UK established the laws of armed conflict, there were a lot of testing and lawyers involved. Therefore, signing the treaty meant taking on a full spectrum of those norms. The laws of armed conflict must apply. It was observed that cyberoperations were very well-planned, tested and controlled because the US signed up for laws of armed conflict. There was scepticism about a large-scale use of cyberweapons due to constraints imposed by international law and norms. It was surmised that large-scale use of cyberweapons was more likely where command and control were not so tight.

PANEL 7: ACTIVISTS, HACKTIVISTS, AND ENTREPRENEURS

The Role of Social Media in Influencing Social Revolution

Muniruzzaman began his presentation with the observation that social media platforms were increasingly utilised by different segments of societies. Some of the main factors that drove the social media communications funnel were socio-economic, political-religious and security concerns.

The pace of growth of social media platforms had been phenomenal. In 2001, Wikipedia was launched. Two years later, it was followed by LinkedIn. In 2004, Google launched Gmail with Myspace and Facebook also coming online in the same year. In 2005, YouTube went live while in 2006, Twitter joined a growing plethora of online communication devices. These social media tools had transformed the way in which humans communicate in a short span of time and the pace of change would continue to accelerate. Prominent characteristics of social media websites included: (a) websites which were "people creating" such as blogs; (b) websites which were "people connecting" such as Facebook and Twitter; (c) websites which were "people collaborating" such as Wikipedia; (d) websites which encouraged reactions such as forums; (e) websites which were "people organising"; and (f) websites which accelerated consumption.

To appreciate the importance of social media, there was a need to understand the changes in the communication landscape. In this age, information was the currency of power and it was evident that states were not at ease in losing their monopoly in this area. Looking at the scale of information consumption, roughly 27 percent of information was being consumed through computers or the internet. The cost of spreading information had also been minimised; any person with a cell phone could become a citizen journalist or photographer, with powerful tools to disseminate news and ideas. Muniruzzaman briefly summarised the general nature and components of social media into 5Ps: (a) "people" who create blogs and various contents; (b) "patterns" which provide feedback; (c) "platforms" such as social networking websites; (d) "processes" which produce user-generated content; and (e) "places" which provide discussion forums.

These tools and platforms provided people with the power to challenge the existing and traditional structures of leaderships. Social media was bringing about an imagined community, enabling many in the fringes of society to take part in social, political and economic discussions. States were frightened of this empowerment and their responses to social media had been negative in general. The empowerment provided by the use of social media however appeared to be a trend that would continue in the coming years.

Contrary to popular belief, the Arab Spring was not the first instance where social media was used extensively in a social revolution. The 2001 ouster of President Estrada in the Philippines saw more than one million text messages exchanged in a week. As a medium, social media was able to empower, engage, update, notify, recruit and delegate followers. It was also a powerful tool in mobilising and coordinating social movements as seen through the worldwide Occupy movement which cut across state boundaries and social statuses. In Kashmir, protestors used social media to distribute information and to organise protests. It had the power to elevate revolutionary icons such as Khalid Mohd Said who became a unifying symbol of the Arab Spring. Muniruzzam concluded by noting that the road ahead appeared to support the continuing growth of social media. He noted that for governments, it was best to embrace and not to fight this trend.

Cyberthreats; Emerging Trends and Various Means Exploited for Cyberfraud and Financial Crime – Are We Doing Enough?

Gunawan Husin's presentation focused on the risk and control mechanisms used by the banking sector in the prevention of new age financial crimes. To underscore the importance and seriousness of preventing financial crimes, Husin recounted that in September 2011, the financial sector in Singapore together with related government agencies conducted a market-wide exercise on cybersecurity. This was a real-time exercise involving around 170 financial institutions and government departments.

Husin commented that there had been an increase in cyberfraud of late, which was mainly due to the low awareness of threats by consumers, and technological advancements that made online fraud easier for criminals, e.g. the invention of skimming devices and scanners that were becoming readily available. Hence, while a lot of new technologies were invented to enhance lifestyles, the risks involved in the use of such technologies must be adequately managed. Accordingly, there were two sources of risks for financial institutions: external criminals and those arising from the conduct of internal staff. As such, on top of "know-your-customer" risk processes, financial institutions were increasingly paying attention to "know-your-employee" profiles. Husin reiterated that there was now greater control over internal processes. Such processes go beyond just checking tick boxes but were actually embedded as business processes in the sector.

For Husin, awareness was of primary importance in fighting online fraud. Fraudsters were going beyond actions taken against bank infrastructures as they presumed that millions of dollars were spent on preventing such occurrences. Instead, more and more criminals were employing social engineering methods. People were primarily the weakest link in online fraud cases. To mitigate the risks of such fraud, banks introduced tools and processes such as RSA security tokens which were used to implement a two-factor identification process.

Husin advocated embedding a strong risk culture in normal business practices. There needed to be strong information policies in place such as not using thumb drives in work computers and drafting stringent social media policies such as uploading pictures of workplaces on Facebook. Other measures involved having robust whistle-blowing policies and a code of conduct for employees who were often the first line of defence against crimes in financial institutions. These were the costs of doing business in the financial sector today. Husin concluded that the above steps should be taken not just for the sake of meeting regulatory compliance procedures and there should be closer cooperation among financial institutions in fighting cybercrimes.

Discussion

Asked whether financial institutions often delay in taking steps to combat fraud due to the cost this would entail, it was stated that banks have different standards of compliance; while some simply want to tick the check boxes, others view the damage to their reputation as being too high a cost to bear and would therefore invest heavily in managing the risks of fraud.

A question was raised whether there would come a time when states intervene and control the content of social media. It was noted that states would like to have some sort of editorial control over social media but this would not be easy as "anti-control" is the very character of social media. It was people-driven and against any sort of formal control. Social media would continue to defy means taken to control it.

Were there problems faced by banks in complying with incident reporting, given that there are risks with internal staff committing fraud? It was explained that with more and more outsourcing by banks, there was a need for banks to address such risks. As such, every line of business in banks was required to perform self-assessments to identify the risks faced and to implement solutions to them. This was something that had to be continuously implemented and monitored to mitigate the occurrences of risks.

PANEL 8: OUTSOURCING CRITICAL INFRASTRUCTURE

Outsourcing Critical Infrastructure: Some Cybersecurity Considerations

Jeremy Chua began his presentation by defining outsourcing as the process of contracting existing business processes which an organisation previously performed internally to an external independent organisation. He stated that organisations outsource for several reasons: (a) to reduce costs and increase savings; (b) to focus on their core business; (c) to access to more knowledge, talent and experience, especially in physical and IT security; (d) to leverage on better best practices; (e) to increase profits; (f) to free up internal resources; and (g) to establish a consistent level of service to the organisation. Electricity generation and distribution, gas production, transport, oil production, telecoms, water supply, agriculture, heating, public health, transportation system, financial services, security services, and IT were examples of services usually outsourced. Chua stressed that it was important to maintain data integrity and security when outsourcing, especially when outsourcing offshore in order to prevent theft or the unauthorised sale of personal data. He believed a company was worth as much as its data.

Chua believed that outsourcing of IT infrastructure was primarily moving to Cloud. He stated that there were several benefits of Cloud despite concerns surrounding the destinations and accessibility of data. Cloud offered flexibility as there was no need for upfront investment in lots of infrastructure, capacity and capital as organisations could add to its cybersecurity infrastructure as it grew. Cloud also offered staff or user access mobility, e.g. "Virtual Machine", Bring Your Own Device (BYOD), and introduced more cost savings with incremental pay-as-you-use payment. Cloud was also highly automated so there was no need to worry about maintenance, upgrading, and skilled or dedicated manpower (headcount), etc. Cloud greatly increased storage and capacity without the extra infrastructure and expense and allowed (under-capacity) IT staff and resources to focus on business rather than infrastructure development. However, organisations should look out for or expect the following risks when outsourcing: (a) unauthorised access to organisation's premises; (b) unauthorised access to organisation's internal IT facilities and information; (c) introduction of malicious codes, e.g. viruses, worms, Trojan horses, trapdoors, etc.; (d) attacks via service provider's systems/networks; (e) non-practice of due diligence on the part of service providers; and (f) inadequate operating processes or procedures. Chua also highlighted some areas of security considerations when engaging or outsourcing cybersecurity functions. Outsourcing organisations should pay attention to: (a) security-related service level requirements; (b) personnel security requirements such as training, certification, and security clearance; (c) information handling; and (d) physical, logical, and electrical access control. Chua concluded by saying that as today's sources of cyberthreats were increasingly hackers, disgruntled employees, hacktivists, cybergangs, terrorists, and that persistent threats were highly advanced, when thinking about outsourcing IT security functions, companies should select the right vendor, and establish the right policies, processes and expectations.

Private Sector Leadership and Empowerment – Multinational Corporations as Global Actors

Jan Neutze began by observing that there was an inherent distrust between the public and private sectors in relation to cybersecurity. Neutze said that the European community wrote approximately 19 drafts of security policy before governments decided to involve the private sector. In 2000, there were not many players in cyberspace, but by 2010, cyberspace had become so crowded that the US, Germany and the UK established

cybersecurity agencies. In 2011 alone, 1.8 zetabytes of data were created. Neutze predicted that by 2020, internet users would have doubled, device proliferation would continue and data volumes would surge 50-fold. Therefore, he stated that it was imperative to consider how consensus could be attained between different stakeholders in relation to cybersecurity.

Policymakers faced new opportunities and challenges in the digital age, for example, Cloud, broadband, social media, global data flows, identity, privacy and security/ policing issues. Effective cybersecurity was a key to success in securing national security while promoting innovation and economic growth, and was emerging as a key issue in international security discussions. Currently, 33 states possessed offensive cyber capabilities, 36 states could develop offensive cyber capabilities quickly, and there had been an increase in sophisticated cyberweapons. The private sector was concerned about the increase in governments' use of cyberweapons, and was uncertain about how international law would prohibit and regulate such use. Potential governmental responses to the militarisation of cyberspace at both national and international levels included regulation, national cybersecurity strategies, military doctrine and capabilities, bilateral agreements and UN-level treaties to limit the proliferation and use of cyberweapons. Potential private sector responses included complying with national regulation, participation in Point-to-Point Protocols (PPP), developing sector plans, crisis management and emergency responses, leveraging best practices for cybersecurity norms and creating industry coalitions.

Neutze argued that norms could be developed more quickly if governments agreed on: (a) Law of Armed Conflict (LOAC) applicability in cyberspace as a baseline; (b) adding underlying internet infrastructure to the list of prohibited targets; (c) protecting the global ICT supply chain; (d) coordinating defence with vendors; (e) respecting non-combatants during a cyberconflict; (f) not abusing private sector technologies; and (g) compensating private sector losses. Neutze then suggested some confidence-building measures: The private sector could contribute to state-to-state confidence-building measures with hotlines, connecting the public sector to existing coordinated emergency response processes for global issues (for example, ICAS), and building government-private sector agreements on triggers or thresholds for such incident response coordination. The private sector could enhance transparency, commit to principles of non-discrimination, and share post-action findings and analysis or remediation plans with the public to protect customers. The desired outcomes of such cooperation would be the government's recognition that the global ICT ecosystem is critical to the global economy and the capacity for constant technological innovation is to be preserved. The public-private process for formulating cybersecurity norms for key areas should be inclusive, and there should be multilateral agreements on accepted behaviour in cyberspace. Finally, national regulations should be mindful of the need for technological neutrality and commercial viability.

Discussion

Asked whether in light that key talents and knowledge were highly mobile, there would be a risk of losing talent, proprietary information and technology as a result of outsourcing, it was stated that in choosing to outsource, the existing policies of the organisation were extended to the third party and there should be some form of agreement, level of comfort and trust between them from the outset. In addition, those who left to join the vendor were usually not focused on the company's core business in the first place.

Were there discussions on political risks, and were reporting to regulators terms written into agreements when outsourcing? It was opined that in Southeast Asia, every governing body or institution had a set of regulations, and with cybersecurity threats, the markets were actually being monitored and trend analyses were being conducted. The problem that the private sector faced was that when governments added regulations, they tended to be very vague. For example, an organisation might be told that it needed encryption without specifying what sort of encryption it needed. Moreover, regulations also rarely specified a deadline for compliance. Therefore, the question to ask was why the government had not done anything about the threats that they already knew about. It was also stated that there had been some considerations, especially in the wake of 9/11, of political and technical risks of outsourcing. For instance, there was consideration to renegotiate service-level agreement (SLA) in the event that governments removed Cloud.

PANEL 9: INTERNATIONAL HUMANITARIAN OBJECTIVES

Human Rights Obligation as a Part of the Global Framework for Cybersecurity: Freedom of Expression

Yu Kanosue began her presentation by describing the roles and functions of the Office of the High Commissioner for Human Rights (OHCHR). The High Commissioner worked directly under the United Nations Secretary-General, and was the second highest office with the responsibility of reporting on human rights issues.

Kanosue explained that states' human rights obligations under the international legal counter-terrorism framework were two-fold: firstly, they had an obligation to prevent terrorist attacks, which had the potential to significantly undermine human rights, and secondly, they had the obligation to ensure all counter-terrorism measures respected human rights.

Kanosue further explained that the legal sources of human rights were spread throughout different international instruments, such as the United Nations Charter (article 55), the Universal Declaration of Human Rights, core human rights treaties and its optional protocols, as well as the Rome Statute. Furthermore, there were various regional instruments as well. The freedom of expression was similarly guaranteed by a number of international and regional instruments. She said that freedom of expression also applied to the internet. This was based on the Human Rights Council's affirmation in its resolution 20/L.13 on 29 June 2012 that the same rights which people had offline must also be protected online, such as the freedom of expression in particular. Restrictions imposed on the freedom of expression must meet the following cumulative criteria: (a) unambiguous law; (b) pursuance of a legitimate purpose, and (c) respect for the principles of necessity and proportionality. There were some forms of expression that states are required to prohibit such as, child pornography, direct and public incitement to commit genocide, advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence, and incitement to terrorism. In the latter context, the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms stated: "An offence to intentionally and unlawfully distribute or otherwise make available a message to the public with the intent to incite the commission of a terrorist offence, where such conduct, whether or not expressly advocating terrorist offences, causes a danger that one or more such offences may be committed".

In conclusion, Kanosue opined that available means to suppress contents deemed to be incitement of terrorism were often "clumsy or ineffective, or both". She suggested using the internet constructively to counter such incitement. For instance, counter-narratives could be disseminated through all relevant media channels, including social networking websites, in order to counter the extremist messages.

The Role of Cyberspace in Promoting Economic and Social Development

Subimal Bhattacharjee observed that when he joined one of the state governments in India 12 years ago, he faced major challenges when discussing cyberissues with older civil servants who did not seem to have a good grasp of cyberspace. He felt that now people had a much clearer understanding of the salient issues related to cyberspace. Today, in India, there were about 140 million users of the internet, and people under the age of 25 constituted 45 percent of these internet users.

In economic and social development, e-government could play an important role. Bhattacharjee explained that around 600 million of the 1.2 billion Indians had passports today. Given the magnitude, the mission mode programme for filing and submitting applications for passports online was a huge endeavour. In terms of e-commerce, e-banking had seen a high increase. Despite the security challenges, consumers seemed to prefer e-banking for convenience and banks also invited their customers to use their websites rather than their actual branches.

Bhattacharjee explained that there were about 45 million Facebook users in India. The apparent challenge was that social media such as Facebook could be used to spread controversial speech. Furthermore, any major controversy or conflict online had ramifications in the real world. In this context, he posed the question what the limits of freedom of speech were. He argued that in a democratic country it was not possible to simply block certain content that might spark conflict in the actual world. Furthermore, there might be a time gap between the publication of a controversial statement and reaction from the government. There might be difficulties and differences in sensitivities that give rise to conflicts, which would make agreeing on laws and regulations very difficult. Internationally, the sensitivities and concepts of acceptable and unacceptable content were even more diverse.

India had benefited greatly both economically and socially from ICT. While in 1998 only about 1.7 percent of the GDP stemmed from the ICT industry, it is roughly 7.5 percent today. In 1998, a few hundred thousand were employed in the ICT sector; today approximately 2.8 million people are employed directly and 8.9 million indirectly. In 1998, exports of ICT products amounted to hardly a few billion dollars; in 2012, it is estimated to add up to roughly 69 billion dollars. Bhattacharjee concluded by remarking that ICT would continue to contribute to the economic and social development in India.

Discussion

Asked whether there were any signatories to the human rights components of the UN Global Counter-Terrorism Strategy, it was pointed out that the UN Global Counter-Terrorism strategy was adopted by the United Nations General Assembly. This meant that it was not a treaty and hence not legally binding. The strategy was regarded as a "soft law", and states were encouraged to use it as a guideline. However, if many states chose to act in accordance with this guideline, the UN Global Counter-Terrorism strategy could be used as a model for future conventions or treaties.

Asked whether this strategy was only applicable to states, or included non-state actors as well, the response was that international laws had traditionally applied only to state actors but this was changing increasingly. The international criminal court, for example, was also looking at crimes perpetrated by individuals.

Lastly, it was mentioned that there was a US court ruling which held that software was a form of expression and therefore protected by the freedom of speech. It was suggested that as 'food for thought', cyberweapons could be regarded as software as well, and as a result, also protected by the freedom of speech.

ROUNDTABLE AND OVERALL POLICY TAKEAWAYS

Panellists presented their views of the future of sovereignty in cyberspace within a timeline of 5 years and 20 years. In general, they believed that there was a need to look at the degree of change in the past to see what would happen in the future. 20 years later, things would become extraordinarily different. The panel argued that changes which could take place in 20 years were vastly underestimated, but overestimated in the coming 5 years.

The role of sovereignty was also debated during the roundtable. Some panellists believed that there would be a stronger role of sovereignty within 5 years, while in the long term, the loss of sovereignty could be expected. Others believed that, 20 years on, cyberspace would see more intense competition than ever before, particularly between internet users and big corporations. Cyberspace would win, but lose out on the potential capacity for debate. They believed that virtual borders will become significantly less unclear over the next few years. There would therefore be attempts to impose borders with law enforcement bodies taking stronger roles.

The role of cyberspace in delivering economic and social benefits in future was also projected by the panellists. They believed that the internet would provide more educational and economic benefits than was previously imagined. Cyberspace would become a venue of innovation for new ideas previously seen as inconceivable.

The intersection between cyberspace and politics was yet another subject of discussion during the roundtable. Some believed that cyberspace would become so vast and dynamic that it would be difficult to conceive living in a state any longer. Cyberspace would become a great levelling field and a great equaliser. Others argued that Parliaments might be a physical entity today, but in the future, people might look towards other forms of reality. For instance, voting through the internet could become a reality in the future.

Panellists also identified possible research agendas in terms of cybersecurity. They believed that this was best done as a government-sponsored initiative, with multiple stakeholders. Four research directions were proposed: (a) common lexicon for cybersecurity that all stakeholders could employ; (b) the ways in which the pros and cons of internet versus non-internet governance could be balanced; (c) developing a just war doctrine to underpin a cyberwar regime; and (d) on the operational level, what the marketplace versus defence standards would be. In the educational arena, training for the next generation of cyberstrategists that blend technological and geopolitical domains of expertise would be important.

Discussion

The discussion centred around China's possible views with regard to the future of sovereignty in cyberspace as well as the contemporary US-Sino cyber and technological race.

One panellist believed that there might be a possibility of Chinese demands for the reinstatement of the UN Code of Conduct when dealing with its own sovereignty in cyberspace. There had been a significant attempt by China to limit the impact of cyberspace to their stability, public safety and economic growth. It was believed that Chinese strategists would most likely continue to work towards protecting their national interests, which could be seen in their current protection of their corner of cyberspace.

Another view was that sovereignty in cyberspace might outlive current expectations. The future model of sovereignty might not provide overall control but would most likely produce effective control. It was also pondered if there would be a different pace of growth for sovereignty. From the national security perspective, those countries that did not move as fast would fall behind in sovereignty. However, it was also possible that those who did not retain sovereignty might be able to interconnect better, innovate better and be more agile than those who did retain sovereignty. The reverse phenomenon might also take place.

A different view was that the West did not have effective countervailing strength against Chinese long-term planning. When the average global growth was 15 percent, US growth was 100 percent; in contrast, China's growth was hovering around 200 percent and tripling in size each year in terms of internet bandwidth ability. However, according to the laws of physics, growth will eventually peter out. This challenged the view that the openness of US society allowed it to innovate better. The US was economically and technologically disadvantaged over the long term because although it funded research, it also allowed research to slip behind for short-term economic benefits. It was concluded that research availed little for the US if it did not know what to capitalise on.

WORKSHOP AGENDA

Sunday, 15th July 2012
Welcome Reception

1700 – 1900hrs	**Arrival of Invited Foreign Participants and Speakers** Venue: Marina Mandarin Hotel
1900 – 2030hrs	**Welcome Reception** Hosted by ***Sean Kanuck***, *National Intelligence Council, Global Futures Forum, US Department of State* and ***Kumar Ramakrishna***, *Head, Centre of Excellence for National Security (CENS), RSIS, NTU* Venue: Aquamarine Restaurant Level 4, Marina Mandarin 6 Raffles Boulevard Marina Square Singapore 039594 Attire: **Casual** (short-sleeved shirt/ polo t-shirt and equivalent attire for women)

Monday, 16th July 2012
Sovereignty Prerogative and International Security

0830 – 0900hrs	**Registration**
0900 – 0915hrs	**RSIS Corporate Video**
0915 – 0930hrs	**Welcome Remarks** by ***Cung Vũ***, *National Maritime Intelligence-Integration Office, Global Futures Forum, US Department of State* and ***Kumar Ramakrishna***, *Head, Centre of Excellence for National Security (CENS), RSIS, NTU* Venue: Vanda Ballroom (Level 5) Attire: **Smart Casual** (Long-sleeved shirt without tie)
0930 – 1015hrs	**Reconciling Westphalia and Cyberspace** Venue: Vanda Ballroom (Level 5) Chairperson: ***Cung Vũ***, *National Maritime Intelligence Center and Global Futures Forum, Department of State* Speaker: **"ICT and Security Developments between 1969 and 2012"** by ***Eneken Tikk***, *Post-Doctoral Fellow at Citizen Lab, University of Toronto; Special Adviser to the ICT4PeaceFoundation, Switzerland*
1015 – 1045hrs	**Tea Break** Venue: Vanda Ballroom Foyer (Level 5)
1045 – 1145hrs	**Panel One – Rules of the Road** Venue: Vanda Ballroom (Level 5) Chairperson: ***Norman Vasu***, *Deputy Head, CENS, RSIS, NTU* Speakers: **"The Proposed UN Code of Conduct in the Realm of Cybersecurity – Balancing Contradictory Goals"** by ***Alan Chong Chia Siong***, *Associate Professor, RSIS, NTU* **"Technical, Legal, and Policy Dimensions of Active Defence"** by ***Herbert S. Lin***, *Chief Scientist, Computer Science and Telecommunications Board, The National Academies*

1145 – 1245hrs

Panel Two – Legal Limitations and Obligations
Venue: Vanda Ballroom (Level 5)

Chairperson: ***Yolanda Chin***,
Research Fellow, CENS, RSIS, NTU

Speakers: **"The Applicability of the Laws of Armed Conflict (a.k.a International humanitarian Law)"** by ***Heather A. Harrison Dinnis***, *Post-Doctoral Fellow, International Law Centre, Swedish National Defence College*

"Identifying the Attribution to a State: The Study of the "Influence" Factor" by ***Setsuko Aoki***, *Professor, Faculty of Policy Management, Keio University*

1245 – 1345hrs

Lunch
Venue: Libra & Gemini Rooms
(Level 1)

1345 – 1530hrs

Panel Three – Potential Domains of Conflict
Venue: Vanda Ballroom (Level 5)

Chairperson: ***Bilveer Singh***,
Associate. Professor, Department of Political Science, National University of Singapore

Speakers: **"Cyberpower: West to East or East to West?"** by ***Rex Hughes***, *Co-Convenor, Cyber Defence Project, Centre for Science and Policy, Wolfson College, University of Cambridge*

"Potential Domains of Conflict: Protecting your Critical Assets" by ***Dagfinn Buset***, *Assistant Director, Norwegian National Security Authority*

"Future Domains of Cyberconflict in the Air, Sea and Space Realm from Japan's Perspective" by ***Motohiro Tsuchiya***, *Professor, Keio University*

1530 – 1630hrs

Breakout Sessions
(Syndicate Sessions to cover topics covered in panels 1 to 3)
Group 1 & 2 : Vanda Ballroom (Level 5)
Group 3: Vanda 4 (Level 6)
Group 4: Vanda 5 (Level 6)

1630 – 1645hrs

Tea Break
Venue: Vanda Ballroom Foyer
(Level 5)

1645 – 1815hrs

Panel Four – Oversight and Administration
Venue: Vanda Ballroom (Level 5)

Chairperson: ***Alan Chong Chia Siong***, *Associate Professor, RSIS, NTU*

Speakers: **"Securing Cyberspace: A Public-Private Shared Challenge"** by ***Ruth David***,
CEO, ANSER

"Maintaining Operability and Resiliency in the Administration of Global Architecture for Cybersecurity" by ***Zahri Yunos***, *Chief Operating Officer, Cybersecurity Malaysia (Ministry of Science, Technology & Innovation)*

"Enhancing Global Cybersecurity Readiness: ITU-IMPACT Case Study" by ***Datuk Mohd. Noor Amin***, *Chairman, IMPACT*

"Introduction to the INTERPOL Global Complex for Innovation" by ***Eugene Soh***, *Head, Project Management Office, INTERPOL Global Complex for Innovation*

1815 – 2100hrs **Dinner Lecture – Geopolitics 2.0**
Venue: Libra & Gemini Rooms (Level 1)

Attire: **Smart Casual** (Long-sleeved shirt without tie)

Speakers: **"Balancing Short and Long Term Cyber Implications"** by ***Andrew Cushman***, *Senior Director, TwC Security, Microsoft Corporation*

2100hrs **End of Day One**

Tuesday, 17th July 2012
Multilateral Internet Governance

0900 – 0930hrs **Registration**

0930 – 1030hrs **Syndicate Group Presentations**
(Issues covered in Panels 1 – 3)
Venue: Vanda Ballroom (Level 5)

1030 – 1200hrs **Panel Five – Setting Standards**
Venue: Vanda Ballroom (Level 5)

Attire: **Smart Casual** (Long-sleeved shirt without tie)

Chairperson: ***Sean Kanuck***, *National Intelligence Officer for Cyber Issues, National Intelligence Council*

Speakers: **"The Role of International Standards and their Impact on the Technology Marketplace"** by ***Goh Seow Hiong***, *Executive Director, Global Policy and Government Affairs, Asia Pacific, Cisco Systems*

"Development of Information Security Standards at the International Level" by ***Chan Kin Chong***, *Chair, Security and Privacy Technical Committee, IT Standards Committee*

"Towards a Trusted Cloud" by ***Aloysius Cheang***, *APAC Strategic Advisor, Cloud Security Alliance*

1200 – 1330hrs **Lunch**
Venue: Aquamarine Restaurant (Level 4)

1330 – 1500hrs **Panel Six – Alternate Governance Models for the Best Cyber Futures**
Venue: Vanda Ballroom (Level 5)

Chairperson: ***Kumar Ramakrishna***, *Head, CENS, RSIS, NTU*

Speakers: **"Existing and Alternate Governance Models"** by ***Jason Healey***, *Director, Cyber Statecraft Initiative, The Atlantic Council*

"Private Sector-Led Governance" by ***Andrew Cushman***, *Senior Director, TwC Security, Microsoft Corporation*

"Balancing Freedom, Security and Sovereignty" by ***Bill Woodcock***, *Research Director, The Packet Clearing House*

1500 – 1600hrs **Breakout Sessions**
(Syndicate Sessions to cover topics covered in panels 4 – 6)
Group 1 & 2 : Vanda Ballroom (Level 5)
Group 3: Vanda 4 (Level 6)
Group 4: Vanda 5 (Level 6)

1600 – 1700hrs **Tea Break**
Venue: Vanda Ballroom Foyer (Level 5)

1700hrs **End of Day Two**

Wednesday, 18th July 2012
Beyond the Nation State

0800 – 0900hrs **Registration**

0900 – 0930hrs **Syndicate Group Presentations**
(Issues covered in Panels 4 – 6)
Venue: Vanda Ballroom (Level 5)

Attire: **Smart Casual** (Long-sleeved shirt without tie)

0930 – 1030hrs **Panel Seven – Activists, Hacktivists, and Entrepreneurs**
Venue: Vanda Ballroom (Level 5)

Chairperson: ***Damien D. Cheong***, *Research Fellow, CENS, RSIS, NTU*

Speakers: **"The Role of Social Media in Influencing Social Revolution"** by ***Maj-Gen. (Ret.) Muniruzzaman***, *President, Bangladesh Institute of Peace and Security Studies*

"Cyberthreats; Emerging Trends and Various Means Exploited for Cyberfraud and Financial Crime – Are We Doing Enough?" by ***Gunawan Husin***, *VP, Global Security and Investigations – Business Resiliency, Singapore, JP Morgan Chase*

1030 – 1100hrs **Tea Break**
Venue: Vanda Ballroom Foyer (Level 5)

1100 – 1200hrs **Panel Eight – Outsourcing Critical Infrastructure**
Venue: Vanda Ballroom (Level 5)

Chairperson: ***Cung Vũ***, *National Maritime Intelligence-Integration Office, Global Futures Forum, US Department of State*

Speakers: **"Outsourcing Critical Infrastructure: Some Cybersecurity Considerations"** by ***Jeremy Chua***, *ASEAN Manager, SECUREAGE Technology Pte Ltd.*

"Private Sector Leadership and Empowerment – Multinational Corporations as Global Actors" by ***Jan Neutze***, *Senior Security Strategist, Office of Global Security Strategy and Diplomacy, Trustworthy Computing, Microsoft Corp.*

1200 – 1330hrs **Lunch**
Venue: Pool Garden (Level 5)

1330 – 1430hrs **Panel Nine – International Humanitarian Objectives**
Venue: Vanda Ballroom (Level 5)

Chairperson: ***Bilveer Singh***, *Associate Professor, Department of Political Science, National University of Singapore*

Speakers: **"Human Rights Obligation as a part of the Global Framework for Cybersecurity: Freedom of Expression"** by ***Yu Kanosue***, *Human Rights Officer, Office of High Commissioner for Human Rights*

	"The Role of Cyberspace in Promoting Economic and Social Development" by ***Subimal Bhattacherjee***, *Country Head, General Dynamics, India*	1600 – 1615hrs	**Tea Break** Venue: Vanda Ballroom Foyer (Level 5)
1430 – 1530hrs	**Breakout Sessions** (Syndicate Sessions to cover topics covered in panels 7 – 9) Group 1 & 2 : Libra & Gemini Rooms (Level 1) Group 3: Vanda 4 (Level 6) Group 4: Vanda 5 (Level 6)	1615 – 1700hrs	**Roundtable and Overall Policy Takeaways** Venue: Vanda Ballroom (Level 5) Chairperson: ***Sean Kanuck***, *National Intelligence Officer for Cyber Issues, National Intelligence Council*
1530 – 1600hrs	**Syndicate Group Presentations** (Issues covered in Panels 7 – 9) Venue: Vanda Ballroom (Level 5)	1700 – 1715hrs	**Closing Remarks**
		1715hrs	**End of Workshop**

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 focused 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	

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 systematic shocks such as diseases and terrorist strikes.*

Homeland Defence

- *A broad domain encompassing risk 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 stress 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 radicalisation 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 ON CENS

Log on to **http://www.rsis.edu.sg** and follow the link to "Centre of Excellence for National Security".

ABOUT RSIS

The **S. Rajaratnam School of International Studies (RSIS)** is a leading research and graduate teaching institution in strategic and international affairs in the Asia Pacific region.

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 teaching 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 Area 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
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 Benny Lim, who is concurrently Permanent Secretary (National Development) and Permanent Secretary (Prime Minister's Office).

NSCS comprises two centres: the National Security Coordination Centre and the National Security Research Centre. Each centre is headed by a Senior Director.

The agency performs three vital roles in Singapore's national security: national security planning, policy coordination, and anticipation of 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, please visit
http://www.nscs.gov.sg

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