Conference Report

RETHINKING INFORMATION AND CYBER WARFARE:

GLOBAL PERSPECTIVES & STRATEGIC INSIGHTS

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

3 March 2014
Traders Hotel
Singapore

CONFERENCE REPORT:

Rethinking Information and Cyber Warfare: Global Perspectives and Strategic Insights

3 March 2014
Traders Hotel, Singapore

Conference report on "Rethinking Information and Cyber Warfare: Global Perspectives and Strategic Insights" organised by the Military Transformations Programme, S. Rajaratnam School of International Studies (RSIS).

TABLE OF CONTENTS

Rapporteur: Michael Raska

This report summarises the proceedings of the conference as interpreted by the assigned rapporteur and editor.

EXECUTIVE SUMMARY

On 3 March 2014, the Military Transformations Programme (MTP) organised a workshop titled: "Rethinking Information & Cyber Warfare: Global Perspectives and Strategic Insights." The workshop focused on the increasingly changing dynamics between national security, defence strategy, information conflicts and cyber operations. In doing so, the workshop addressed the emerging theoretical and conceptual debates underscoring cyber conflicts, the political, legal, and technological context shaping information operations and cyber warfare, and a range of case studies of how selected states are conceptualising cyber warfare in their strategic thought, defence planning, and operational conduct.

Acknowledging the need to examine cyber conflicts and cyber security through multi-level, inter-disciplinary, and international perspectives, the workshop brought together renowned scholars in strategic studies, policy experts, defence planners, information technology experts, and business leaders from the United States, Germany, Israel, United Kingdom, Switzerland, Japan, Australia, and Singapore. No single, overarching consensus emerged on the strategic implications of cyber warfare. Instead, the discussions demonstrated the enormous complexity of the issue. The discussions also demonstrated significant nuances in the perceptions, strategies, and responses to varying cyber threats – many of which are captured in this report.

Ultimately, cyber security will increasingly shape both military and technological futures. RSIS Military Transformations Programme promotes greater understanding in this area. At the same time, the idea of bringing together Asian, European, American, and Australian scholars to discuss cyber security in the broader context of strategic studies fulfilled one of the key strategic goals of RSIS: to form a global network of excellence in national security, defence and strategic studies, diplomacy and international relations.

INTRODUCTORY ADDRESS

Dr Michael Raska, Research Fellow in the RSIS Military Transformation Programme, highlighted the strategic significance of the on-going information revolution and progressive complexity of cyber threats, which are increasingly blurring distinctions between civil and military domains, state and non-state actors, principal targets and weapons used. As more governments, intelligence agencies, military organisations as well as non-state actors invest in developing cyber capabilities, he argued that future conflicts will be increasingly linked with confrontations in and out of cyber space, cyber attacks on physical systems and processes controlling critical information infrastructure, information operations, and various forms of cyber espionage.

The continuously evolving multi-dimensional character of information and cyber operations enables new types of "force multipliers" – the ability to operate rapidly against distant adversaries without the commitment of combat personnel; the ability to act in secret by minimising exposure, attribution, and subsequent risks of counter-attacks, the ability to use cyber weapons as disrupt, deny, destroy, or subvert key nodes of critical national infrastructures, including communications systems, banking and finance, logistics and transportation systems, national databases, and other vital information grids.

In this context, the conceptual development of information and cyber warfare has evolved parallel with the diffusion of global information revolution in the military domain over the past three decades. Notwithstanding the use of electronic warfare in combat since the Vietnam War and the Yom Kippur War, the first wave of cyber/information warfare began in the early 1990s when the United States military experimented with "defensive information operations" vis-à-vis Iraq during the Gulf War, which gave the U.S. military an edge in battlefield intelligence, targeting and command and control.

From the mid-1990s, a second wave emerged with the considerable developments in computer and communications technologies, which sparked a conceptual debate on future conflicts in the information age. While the information warfare debate was still confined primarily to the military domain, particularly with emerging concepts such as "cyber wars" and "net wars" in both offensive and defensive modes, its scope gradually included aspects of intelligence-based warfare, economic warfare, cyber warfare and hacker warfare that provided individuals, state and non-state actors with unparalleled capabilities to deny, disrupt, deceive and destroy information systems and environment.

Currently, we are in the third wave of "computer network operations" that combine select elements of cyber and information warfare, including information denial, disruption, destruction and manipulation campaigns, confrontations in cyber space, attacks on computerised systems, cyber attacks on physical infrastructure systems, cyber espionage, electronic warfare, strategic communications and perception management. The key questions for the debate include whether and how will the use of force change with the next wave of "weapons of mass effectiveness" embedded in future projections of cyber warfare? In this context, what do we mean by "power projection" in the 21st century? What is the relationship between "hard" and "soft" power in the context of cyber conflicts? How will cyber warfare impact strategic theory?

PANEL 1
Theorising Information and Cyber Warfare: Intellectual History, Concepts, and Debates

Cyber War, Cybered Conflict and the International System

Dr Peter Dombrowski, Professor of strategy at the U.S. Naval War College, began the first panel on the theoretical and conceptual history of cyber conflicts and their relevance for East Asian security. Presenting a paper co-authored with Chris Demchak, Professor of Strategic Research at the U.S. Naval War College, he argued that over the last two decades, political leaders, general officer and civilian strategists have struggled to understand the impact of cyber space on conflict and war. According to Dombrowski and Demchak, the U.S. military termed cyber space as a separate military domain in line with traditional war fighting concepts tied to the air, land, sea, and even nuclear domains. However, cyber space as a separate domain has been too narrow a term for understanding the global, complex digital system that transcends boundaries of land, sea, air, institutions, and nations.

In other words, the importance of cyber space in conflict is not whether computer networks are involved as a separate domain, but where, how, and to what significance they have for strategic outcomes. Accordingly, they suggest conceptualising the term "cybered" conflict, defined as any conflict of national significance in which success or failure for major participants is critically dependent on computerised key activities along the path of events. The term "cybered conflict" means that all adversarial and competitive relationships will have a cyberised dimension. As all modern systems, from finance to transport, require telecommunications and computers connected to the Internet or proprietary networks, different adversaries will seek to influence outcomes by accessing and altering both the systems themselves and the data that resides within.

For militaries, boots on the ground and ordinance on targets may be the ultimate determinants of victory, but deploying soldiers in the field or launching missiles requires the secure, accurate, and timely flow of information. Therefore, developing cyber defences will be a necessary, but not sufficient factor. As new threats emerge, including internal threats from formerly trusted agents, government agencies and military organisations will have to increasingly build in redundancies, while avoiding single points of failure. Building resilience in turn will depend on the capabilities of talented, well-trained personnel able to respond quickly to repair, restore, and re-build.

Mastering "cybered conflict" will be a long and likely painful process. Technologies evolve rapidly; developing defensive and resilient institutions remains a game of catch up. States will try to regulate and govern but will often fail or get things wrong. Gains to be made from cyber exploits – whether stealing intellectual property or disabling military equipment used for in a shooting war or deceiving publics with misinformation transmitted over social media – are simply too great for ambitious generals, corporate buccaneers, and criminals to resist.

The Intellectual History of Cyber Warfare: from Advancing Sovereignty to Strategy Contra-Sovereignty

Dr Alan Chong, Associate Professor at the S. Rajaratnam School of International Studies, presented a paper on the evolving intellectual history of cyber warfare through the lens of five schools of thought: (i) strategy of warfare as mind reading the opposition; (ii) sentient war in the electronic global village; (iii) electronic Pearl Harbour; (iv) the soft power of open seduction; and (v) patriotic and autonomous hackers. Applying an inter-disciplinary perspective based on political science and sociology, Chong argued that cyber warfare cannot be discussed without involving analysis of the operation of power in and of the state. In this regard, the intellectual history of cyber warfare can be seen as a conceptual struggle by its interpreters in the broader context of "sovereignty."

According to Chong, cyber warfare remains a new theoretical frontier in relation to Strategic Studies, Security Studies, and International Relations. It has opened up connections with existing literatures in strategic thought, while also drawing upon international studies of the impact of digital technologies on global transformations. A good deal of the intellectual history, nonetheless, affects sovereignty and its powers invested in statehood. Digital frontiers have opened up the protection of the sovereign national interest, and efforts or 'strategies' – to perforate, or penetrate sovereignty from its outside and inside as well.

The key question is whether we are entering a realm of the ultimate technological levelling in strategy, privileging both state and non-state actors? The policymaker and state-linked political analyst will argue for sovereignty, but the individual living in the electronic global village will have a range of new choices. In this regard, the intellectual history of cyber warfare should awaken new research on "cyber politics" - to actively draw upon social scientific methodologies and insights in order to supplement the study of what is clearly more than just a computer engineering problematique.

Cyber Conflicts and the Future of Asian Security

Dr Benjamin Schreer, Senior Analyst for Defence Strategy at the Australian Strategic Policy Institute (ASPI), argued that it is important to introduce some caution into the Asian debate on "cyber conflicts." The emerging strategic debate points to serious limitations regarding the use of the cyber domain for political purposes, particularly at the higher end of the conflict spectrum. "Cyber warfare" in itself, according to Schreer, seems ill-suited as a tool of coercion or deterrence. As a consequence, cyber space per se does not increase the likelihood of major escalation in Asian 'hot spots' such as the Korean Peninsula, the Sino-Japanese dispute, or the Taiwan Straits. It is also not entirely clear that cyber espionage and sabotage will yield countries a significant strategic advantage.

In this context, Schreer argued that contrary to the prevalent view that cyber warfare will be a defining feature of East Asia's future strategic landscape; it is not clear how cyber conflicts will actually shape Asian security. In his view, the conceptual drive in defining "cyber conflicts" should be viewed through the lens of political conflicts in which states use "cyber means" to settle or influence a conflict. In other words, the key question is how does the use of "cyber space" help states in East Asia to achieve political or strategic objectives? What can we say about cyber warfare and cyber espionage as tools to solve regional political disputes? The strategic and analytical community has barely started to think about the challenges related to cyber warfare and cyber conflicts, for example in terms of battle-damage assessments and attribution.

Moreover, there is a lack of consensus in how to characterise the strategic instabilities between states caused by cyber interactions, and what to do about it. Cyber warfare thus does not represent a new form of Revolution in Military Affairs – it does not transform regional power structures, it does not replace the military capabilities of the most advanced powers in the region, and ultimately, it has a limited utility to achieve desired political outcomes. Simultaneously, the lack of attribution amplifies its limitations both as a means of deterrence or coercion. While the uncertainties related to the effects of cyber attacks coupled with the possibility of undesired escalation could actually induce an element of restraint in major power relations, they also undermine the "cult of the cyber offensive." Cyber warfare, in short, is not a major threat to strategic instability between major powers, particularly the U.S. and China, now will alter significantly the regional balance of power. Cyber warfare capabilities can only strengthen the already strong militaries in the region, complementing the traditional forms of the use of force.

Tackling Emerging Cyber Threats: Cross-sectoral Perspectives

Changing Dynamics of Cyber Threats: Legal and Political Contexts

Shifting the discussion towards the changing political, legal, as well as technological dynamics of cyber threats, **John Bassett OBE** (Royal United Services Institute) shared lessons learned from his two decades of service at the U.K.'s GCHQ. He noted the increasing level and sophistication of cyber attacks, and the challenges for governments in their efforts to devise effective cyber defence. Specifically, Bassett focused on four pressing challenges: (i) the corrosion of wider international relations caused by the increasing proliferation and deployment of cyber weapons; (ii) the need to maintain the right balance between security and civil liberties in the aftermath of recent revelations by Wikileaks; (iii) the need for an effective approach to supply chain security that meets both security and economic requirements; and (iv) the need to develop far better understanding of cyber threats in government, military and business leaders, and wider civil society.

Bassett offered his perspective on the future of cyber conflicts and cyber security. By 2020, intelligence agencies will not be talking about cyber security under existing notions and preconceptions. Rather, there will be a developing merger between those aspects currently considered as cyber security and new forms of robotics and artificial intelligence embedded in the "Internet of Things." The threat matrix, however, will be similar based on the convergence of human aspects (i.e. insider threats), supply chain threats, electromagnetic weaponry, and other threats. On the operational side, the massive proliferation of cyber weapons will preclude the governance of covert operations – from issues of access to verifications, which may have negative repercussions on the conduct of international relations. There will be also an increasing need to maintain public support and consent in the conduct of intelligence agencies in the world of cyber space. Ultimately, the concepts, strategies, processes, and organisations will shift from cyber risk-avoidance to cyber risk-management in diverse areas such as the selection of staff, evaluation of security procedures, and supply chains.

Protecting Critical National Infrastructure: Lessons Learned

Dr Doron Zimmermann, Senior Manager Security Affairs at Swissgrid Ltd. - Switzerland's national transmission system operator, provided insights on protecting critical national infrastructure based on lessons learned through the evolving public-private partnerships in Switzerland. He noted that the integral protection of critical assets, processes and people operating critical infrastructure constitutes a key priority in national security deliberations, particularly as advanced economies are centralising core service functions – from energy, transportation, finance, medical services, to communications, data storage, and operation of water as well as sanitary facilities. He argued that the principal means in the critical infrastructure protection (CIP) endeavours is not a single measure, but rather a collaborative approach by which all necessary protective measures are identified and implemented in accordance with an integral approach to security.

In his presentation, Zimmermann highlighted a new phenomenon: complex inter-dependency. One of the key material components of the complex inter-dependent systems linking continents, states and their economies is critical infrastructure such as health, financial, IT, security and energy sectors. As the spectre of extreme asymmetrical conflict looms large – a single individual´s use of deadly technology can conceivably compel a government, or a number of governments co-dependent upon each other´s critical infrastructures. In many advanced societies, the one critical infrastructure element that pervades all others is energy: from lighting to petrol pumps, from powering medical facilities to the operation of sanitary facilities. The transport of bulk energy represents the most vulnerable and potentially highest impact target.

Notwithstanding more mature CIP Public Private Partnerships in the U.S. or U.K., the Swiss example is an apt one, demonstrating that multiple government stakeholders show a clear and sustainable interest in securing one of the most critical national infrastructures.

PANEL 2

Emerging Cyber Threats: A 'White Hat' Hacker's Perspective

Fabrice Marie, founder of Kibin Labs Ltd. - one of the leading Cloud computing professional service consultancies in the Asia Pacific region, shared his insights based on life-long experiences as a 'white-hat' hacker. Marie focused on the future of hacking and its different branches - attacks perpetrators, targets, team sizes, motivation as well as sponsors. He outlined the varying motivations, trajectory, magnitude and impact of different hacker actors: from an almost harmless geek hobby, to a full-blown industry with its benefactors and black sheep. In doing so, he argued that organised crime, governments and large corporations are all turning to hackers for select covert operations. Marie also shared his views on the potential targets – increasingly inter-dependent critical national infrastructure systems.

The present and future of hacking, according to Marie, is and will be played on the public and private clouds, as almost everything is already on clouds and governments are aggressively adopting cloud technologies and automation systems that completely disregard security, let alone government grade or military grade security. Since cloud is ineluctable and automation is ineluctable for large clouds, he recommends one of two approaches: either automating large heterogeneous secure clouds or the better option to automate homogeneous "trusted operating systems" using software stacks such as SELinux or RSBAC and proper automation framework. Trusted operating systems have been shunned because of their management complexity, but Marie argues that a properly coded and configured automation system could take care of that burden and manage "trusted clouds."

PANEL 3

Cyber Security and Defence Strategy – Country Perspectives (1)

Russian Perspectives on Cyber (Information) Warfare

Dr Dima Adamsky, Associate Professor at the Lauder School of Government, Diplomacy and Strategy at the Interdisciplinary Center in Herzliya, Israel, examined key concepts and notions about the impact of cyber capabilities on the character of warfare that have been circulating in the Russian strategic and expert communities over the last decade. He situated Russian approaches in the comparative context of the global competition of cyber learning, and the intellectual sources of Russian thinking about information (cyber) warfare. Adamsky highlighted three unique characteristics in the Russian approach: "holism," "hybridity," and "permanency."

Russian approach is qualified as holistic since in cyber offence and defence operations it attributes equal importance to "hostile code" and "hostile content," and merges between the two. Info-technical strikes and info-psychological pressure, according to this approach, are dialectically inter-connected. Syntactical attacks (disrupting information system by malicious code) and semantic attacks (destructing decision-making process by manipulating the contents) are part of the same operation. Hence, digital sabotage (disorganise/disrupt/destroy state's administration capabilities) and psychological subversion (discredit leadership, disorient operators, demoralise population) to coerce the actor to make decisions in the interest of the other side, are two parts of the integrated cyber whole. Consequently, according to the holistic approach "means of information struggle," are also multi-disciplinary and include computer network operations (CNO), electronic warfare (EW), psychological operations (PSYOPS), and camouflage, concealment and deception (CC&D).

Russian approach can be qualified as unified and hybrid because of the quest to synchronise efforts across several domains: IW operations, kinetic campaign, battle of narratives and public diplomacy are waged simultaneously as one campaign. Online events/narratives trigger off-line events/behaviour and vice versa, so that eventually the operational effects across the domains are orchestrated and synchronised. The cumulative effect is achieved, among others, by the unity of various actors involved. Modus operandi is hybrid since various state and non-state cyber actors and capabilities are co-opted and coordinated by the invisible hand.

Finally, the permanency of cyber efforts across space and time characterises Russian approach. IW campaign does not have clear beginning and clear end and does not differentiate between "strategic time zones." It is a continuous multi-dimensional campaign conducted in peacetime, in the prelude to war and in wartime. It takes place in uninterrupted manner on all three levels of activity: tactical, operational and strategic, with the varying level of escalation and varying ratio of psychological and digital pressure according to the circumstances. Time perspective of such campaign is much longer than in the West as it is not confined to particular crisis or event.

Chinese Approaches to Cyber Warfare

Dr Jon Lindsay, Research Scientist at the University of California Institute on Global Conflict and Cooperation (IGCC), reflected on the Chinese approaches to cyber warfare. He observed that cyber security issues have become a major source of tensions in the U.S.-China relations - Western pundits and policymakers often single out Chinese hackers as a major threat to economic and national security. Chinese critics, by contrast, decry the United States' outsized influence over the internet, demonstrated use of cyber weapons against its adversaries, and alleged leverage over major firms like Facebook and Google for intelligence collection. This unfortunate situation exacerbates mistrust and raises suspicions in both countries regarding the others' motives and activities.

To get beyond the hype, Lindsay argued, an understanding of China and cyber security requires a combination of international and inter-disciplinary perspectives. Contrary to popular perceptions in the United States, China does not have a monolithic, coordinated policy approach to cyber security. Although political power is centralised in the Chinese Communist Party, Chinese governance is fragmented regionally and functionally. For civilian or industrial cyber security, China has to contend with a complicated tangle of regulatory institutions, inconsistent implementation of policy directives, and public and private sector actors pursuing incompatible interests. At the same time, there is a fractious network of military, intelligence, and other state entities involved in cyber policy and activity who are concerned about international as well as domestic security.

There has been vigorous debate in Chinese defence intellectual circles about the nature of information warfare, inspired by a number of different influences, sometimes similar to perspectives of other nations, and sometimes unique to China. As in the civilian cyber security sector, the implementation of these ideas by various military, intelligence, and civilian militia organisations is not systematically integrated.

Ultimately, China's influence in cyber space parallels its meteoric economic growth and formidable military transformation. Notwithstanding the extensive political and industrial espionage originating from China, such activities may not enhance relative Chinese competitiveness, and may even impede China's long-term growth trajectory. As a result, unilateral action by states to protect themselves from threats both real and imagined could undermine the productivity of the global internet. The real threats to the efficiency of cyber space should not be conflated, however, with overhyped fears of Chinese cyber security prowess.

From Start-up Nation to Cyber Nation – The Israeli Case of Cyber Security

Ram Levi, cyber security expert and founder of Konfidas Ltd., presented his views on the continuity and change in Israel's cyber security policies, and efforts of various governmental organisations in Israel to protect cyber space. Levi argued that the increased dependency on cyber space requires protecting computer systems that are vital to daily life. Many areas in the public and private sectors are vulnerable to a cyber attack: hospitals, national databases, electric and water grids, telephone networks, Internet servers, banks, government offices, businesses, national security and cyber space systems, and even PCs and mobile phones. All of these areas need protection.

In 2010, a National Cyber Taskforce was established in Israel to guarantee Israel's global leadership in cyber space and provide the best possible defence for the country's cyber infrastructure. The taskforce dealt with the question – how to maintain Israel's position as a global leader in the development of information technology, and what are the steps that need to be done for Israel to acquire state-of-the-art cyber capabilities to protect its economy, while preserving its open, democratic, knowledge-based society.

Due to the unique nature of the existing and anticipated challenges, an inter-disciplinary and multi-disciplinary approach to protect cyber space is needed. Israel's cyber leadership vision can be only realised through a national programme. The state is investing in its digital future to meet the challenge of future cyber threats. This requires systematic handling, regulatory and legislative changes, increased budgets, and coordination and cooperation between businesses, academia, and the defence establishment.

Cyber Security and Defence Strategy – Country Perspectives (2)

Japan's Cyber Security Issues, Challenges, and Responses

Mihoko Matsubara, Cyber Security Analyst with Hitachi Systems, Ltd., Tokyo, elaborated on the unique cyber security challenges facing Japan, which she argued are compounded by complex factors embedded in Japanese cultural and historical experiences. In particular, Japan traditionally did not attach sufficient weight to security strategies, and its attitude to the darker aspects of the country's antebellum history and current pacifist constitution have served to curb appreciation of robust use of intelligence and security services, including those related to cyber security. Even though other countries such as the United States have started, if in piecemeal fashion, to realise the necessity of holistic approaches to cyber threats and human-driven risks, Japan still leans towards technical solutions and its responses tend to be reactionary.

Matsubara noted the nature of the information revolution has created two universal cyber security issues with which the world's governmental and private-sector actors must contend: invisible, ostensibly unpredictable risks and the necessity of cross-sectoral cooperation.

First, cyber attacks are not necessarily visible, which makes it challenging to assess or minimise damage such as information leaks. The level of sophistication of some cyber espionage campaigns is enough to remain undetected for months or even years. This stealthy nature of cyber attacks aggravates efforts, governmental or otherwise, to counter them. Second, such a broad spectrum of reliance on information networks and their attendant risks empower multiple governmental organisations to lead national cyber security efforts, especially regarding initiatives related to the protection of critical infrastructure. Critical infrastructure itself, however, necessitates that several agencies or ministries take responsibility for regulatory or security oversight. Furthermore, culprits can launch cyber attacks regardless of national borders.

Thus, cyber security efforts require cross-sectoral and international cooperation to counter or mitigate threats. However, internal turf battles and bureaucratic stovepipes occlude collaboration in developing and implementing overarching policy. Since the Japanese government struggles with cyber security internally, it is also more difficult to work together with other nations whose stakeholders may have different perspectives, interests and priorities.

As cyber attacks are becoming more sophisticated and abundant, and while the Japanese workforce is decreasing, safety and security are no longer free. The country can afford no further delay in incorporating cutting-edge cyber security procedures into their daily business practices and in integrative learning about the myriad aspects of cyber security, not only technical but also geopolitical and legal ones. It will also be crucial to revise immigration standards and to promote international partnerships with foreign firms in order to secure relevant expertise and manpower. Such are the first steps, Matsubara argued, that Japan should take to overcome its cultural and historical barriers and enhance its cyber security, though many more will follow.ones. It will also be crucial to revise immigration standards and to promote international partnerships with foreign firms in order to secure relevant expertise and manpower. Such are the first steps, Matsubara argued, that Japan should take to overcome its cultural and historical barriers and enhance its cyber security, though many more will follow.

U.S. Perspectives on Cyber War

Dr Tim Junio, Cyber Security Fellow at Stanford University, posed the question: "Is there an American way of cyber war"? By a "way of cyber war," he means how militaries train and equip to fight, as measurable in acquisitions, training, doctrine, and other aspects of readiness. He argued that at the highest levels of abstraction, U.S. Department of Defense bureaucracies have measurable preferences for strategy, organisation, and procurement related to cyber operations that differ from those of other U.S. bureaucracies (such as law enforcement and homeland security) and from the militaries of other countries. This constitutes a theoretical and empirical finding of interest: militaries vary in how they plan to conduct cyber operations, and cyber "wars," should they ever occur, are highly unlikely to look the same around the world.

Measuring a "way of war" is highly complicated, and Dr Junio offered a partial explanation of how the U.S. military plans for cyber conflict along five dimensions that are measurable between bureaucracies and between countries. The first is a preference for offensive operations, particularly preemption and retaliation. Dr Junio concludes, based on interviews and newly available primary source documents, that the U.S. Department of Defense has far greater faith in the military expediency of offensive cyber operations than any other U.S. Government bureaucracy.

Second, Dr Junio argues that the U.S. military treats "all special operations as cyber operations." That is to say, operations are highly technical and emphasise the creation of small cadres of well-equipped and exceptionally-trained experts. This is linked to the third U.S. way of cyber war, which is to obsess over technological superiority at the cost of scale. For example, he noted that for the United States, a significant uptick in the production of cyber military forces – approximately 4,000 personnel – is almost irrelevant relative to the scale of cyber operations among the United States' competitors. Credible sources report, for instance, that the number of cyber operators taking direction from China's military is well over 100,000. The finding regarding the United States is different from what one might expect deductively; information technology allows for stealthy and low-cost operations that may be scaled easily, cyber crime being an excellent example, rather than require large infrastructure and experts to achieve effects.

Fourth, the U.S. military domain for cyber operations is highly circumscribed, and these parameters are effectively drawn by a combination of statute, policy, and organisational culture. The primary U.S. military mission is to equip, plan, and prepare for cyber operations as part of military conflict and/or as independent offensive operations, and these responsibilities are distinct from law enforcement or homeland defense missions, which are handled by other parts of the U.S. Government. This differs sharply from many other parts of the world, and from other policy domains in the United States, as protecting the U.S. from many types of foreign aggression are considered "defence" rather than "homeland security" functions.

Finally, the United States has centralised the organisation of capabilities and training for its cyber operations. This is surely a variable, in that other kinds of military activity delegate decision-making downward, and it is not clear a priori whether or not a service would concentrate all effective power in the homeland (as the United States has done with Ft. Meade) versus generate cyber forces as components to all existing forces, which in the United States might look like cyber units in each combatant command. The U.S. solution appears to be sending forces from the centralised unit (Cyber Command) to forward areas (combatant commands), though the long-run result remains to be seen. There is as-yet no U.S. military equivalent of a cyber warfare platform akin to an assault rifle, or fighter plane, or aircraft carrier.

Despite these American ways of cyber war, important aspects are not yet established, particularly related to the operational and tactical levels of war. Bureaucratic conflict persists among the military services, which duplicate many activities, and between the armed forces and intelligence bureaucracies in the Department of Defense, which perceive a benefit from eavesdropping on functioning networks rather than focus on degrading adversary networks. In the coming decades, many of the identified practices will become institutionalised, and as more data become available on foreign military cyber warfare activities, a more comprehensive comparative perspective will allow scholars to yield greater insight into how organisations are adopting this new set of technologies.

Australia’s Cyber Security Strategy

Dr Tobias Feakin, Director of the International Cyber Policy Centre, and Senior Analyst for National Security at the Australian Strategic Policy Institute (ASPI), noted that cyber security has rapidly emerged as a high-priority policy challenge for the Australian Government, mirroring wider international concerns around escalating levels of malicious online activity. He argued that Australia’s cyber policy has largely failed to keep pace with these recent developments. The government’s centre-piece “Cyber Security Strategy” is now five years old and in need of urgent revising. In this context, Feakin examined Australia’s cyber security organisational structures and noted key issues within these. He also examined the Asia Pacific regional context in which Australia sits and how the government is responding to challenges inherent to the region. He concluded with an assessment of how these government efforts have been challenged in the Snowden era and identified potential pathways to substantive international dialogue through the debris of the Snowden affair.

In this context, Feakin noted that the ability to leverage cyber space has become one of the twenty first century’s most important sources of power. State and non-state actors can use this power to achieve financial, military, political, ideological or social objectives in cyber space or the physical world, to positive or negative ends. Like most technologies, cyber space is agnostic to politics and ideology, but is a powerful transfer mechanism for both. The twenty first century is going to be defined by the cyber domain. There will be a great responsibility to ensure that those that wish to exploit cyber space for negative purposes are denied as much operating space as possible. This must be achieved without reducing the openness and freedom that the cyber domain has enabled.

However, due to the sheer number of different stakeholders in the cyber domain, policy solutions are going to require cooperative approaches which accommodate—where desirable—the various interests of those groups. But cooperation is difficult to achieve at present because of the significant divergence in behaviours at individual, national and international levels. In relation to state behaviour, there’s enormous variance in the ways states approach cyber space even within their own jurisdiction and this affects the way in which their citizens and private companies are able to interact with it. There’s also great diversity in how countries use cyber as a tool of external policy, with applications as wide ranging as business, espionage, war fighting or for development aid. Understanding these challenges and creating innovative solutions will be essential for government and private sector alike.

As key policy recommendations, Feakin noted the need to generate policy commitment for Australia to cooperate with allies and partners to promote norms of behaviour in cyber space, including delivering capacity building initiatives around the region, and developing bilateral and multilateral agreements on cyber security. Feakin proposed harmonising the varying legal frameworks such as the Budapest Convention (2013), UN Group of Governmental Experts, and ASEAN Work on Confidence Building Measures (2014). In sharing approaches to cyber policymaking, there is more room for transparency, training and simulation for crisis management and incident response, raising technical and policy standards, and engaging the private sector in joint capacity building, particularly in sharing threat data and best practices.

PROGRAMME

0830 **Registration**

0900 **Welcome & Overview**
Michael Raska
S. Rajaratnam School of International Studies (RSIS),
Nanyang Technological University

0910 **Panel 1**
Theorising Information and Cyber Warfare: Intellectual History, Concepts, and Debates
Chair:
Pascal Vennesson
S. Rajaratnam School of International Studies (RSIS),
Nanyang Technological University

Cyber War, Cybered Conflict and the International System
Presenter:
Peter Dombrowski
Naval War College

The Intellectual History of Cyber Warfare: from Advancing Sovereignty to Strategy Contra-Sovereignty
Presenter:
Alan Chong
S. Rajaratnam School of International Studies (RSIS),
Nanyang Technological University

Cyber Conflicts and Asian Security
Presenter:
Benjamin Schreer
Australian Strategic Policy Institute

Q&A Discussion

1030 **Tea/Coffee Break**

1045 **Panel 2**
Tackling Emerging Cyber Threats: Cross-Sectoral Perspectives
Chair:
Caitriona Heinl
S. Rajaratnam School of International Studies (RSIS),
Nanyang Technological University

Changing Dynamics of Cyber Threats: Legal and Political Context
Presenter:
John Bassett OBE
Royal United Services Institute

Emerging Cyber Threats: A 'White Hat' Hacker's Perspective
Presenter:
Fabrice Marie
Kibin Labs

Protecting Critical National Infrastructure: Lessons Learned
Presenter:
Doron Zimmerman
SwissGrid

Q&A Discussion

1215 **Lunch**

1330 **Panel 3**
Cyber Security & Defence Strategy (1)
Chair:
Bernard Loo
S. Rajaratnam School of International Studies (RSIS),
Nanyang Technological University

PROGRAMME

Russian Perspectives on Cyber Warfare
Presenter:
Dima Adamsky
The Interdisciplinary Center Herzliya

Chinese Approaches to Cyber Warfare
Presenter:
Jon Lindsay
Institute on Global Conflict and Cooperation, University of California San Diego

From Start-up Nation to Cyber Nation – The Israeli Case of Cyber Security
Presenter:
Ram Levi
Tel-Aviv University

Q&A Discussion

1500 **Tea/Coffee Break**

1545 **Panel 4**
Cyber Security & Defence Strategy (2)
Chair:
Richard Bitzinger
S. Rajaratnam School of International Studies (RSIS),
Nanyang Technological University

Japan's Cyber Security Issues, Challenges, and Responses
Presenter:
Mihoko Matsubara
Hitachi Systems

U.S. Perspectives on Cyber Warfare
Presenter:
Tim Junio
Stanford University

Australia's Cyber Security Strategy
Presenter:
Tobias Feakin
Australian Strategic Policy Institute

Q&A Discussion

1715 **Review and Closing Remarks**

BIOGRAPHY OF SPEAKERS

Dima Adamsky

Dima Adamsky is Associate Professor at the School of Government, Diplomacy and Strategy at the IDC Herzliya (Israel). He has been a pre- and post-doctoral fellow at Harvard University and a visiting fellow at the Institute of War and Peace Studies, Columbia University. His research interests include international security, strategic studies, cultural approach to IR, modern military thought, nuclear strategy, American, Russian and Israeli national security policy. He has published on these topics in Foreign Affairs, Journal of Strategic Studies, Intelligence and National Security, Studies in Conflict and Terrorism, Journal of Cold War History, Defence and Security Studies. His books Operation Kavkaz and The Culture of Military Innovation (Stanford UP) earned the annual (2006 and 2012) prizes for the best academic works on Israeli security. In addition to his academic career, in his positions in the Israeli MoD and the IDF, Dr Adamsky has carried out intelligence analysis and strategic policy planning. In the latter capacity, he served as assistant secretary of the committee charged with formulating Israel's national security concept.

John Bassett OBE

John Bassett is a Director of Dianoia Consulting Ltd and an Oxford Martin Associate advising on cyber policy and defence at the Global Cyber Security Capacity Centre at the University of Oxford. His current interests include low intensity cyber warfare and its consequences, the human dimensions of cyber security and effective preparation to deal with cyber attacks. In 2010 he became the first Fellow for Cyber Security at the Royal United Services Institute in Whitehall, London. John Bassett served in GCHQ from 1991 to 2010 in a range of operational posts at home and overseas. John Bassett was educated at Bristol Grammar School, Oxford University (MA in Classics) and the University of the West of England (MSc in Information Technology). Her Majesty, The Queen appointed him an OBE in 2003.

Alan Chong

Alan Chong is Associate Professor at the S. Rajaratnam School of International Studies in Singapore. He has published widely on the notion of soft power and the role of ideas in constructing the international relations of Singapore and Asia. His publications have appeared in The Pacific Review; International Relations of the Asia-Pacific; Asian Survey; East Asia: an International Quarterly; Politics, Religion and Ideology; the Review of International Studies; the Cambridge Review of International Affairs and Armed Forces and Society. He is also the author of Foreign Policy in Global Information Space: Actualizing Soft Power (Palgrave, 2007). He is currently working on several projects exploring the notion of 'Asian international theory'. His interest in soft power has also led to inquiry into the sociological and philosophical foundations of international communication. In the latter area, he is currently working on a manuscript titled 'The International Politics of Communication: Representing Community in a Globalizing World'. In tandem, he has pursued a fledgling interest in researching cyber security issues. He has frequently been interviewed in the Asian media and consulted in think-tank networks in the region.

Peter Dombrowski

Peter Dombrowski is a professor of strategy in the Strategic Research Department at the Naval War College. Previous positions include chair of the Strategic Research Department, director of the Naval War College Press, editor of the Naval War College Review, co-editor of International Studies Quarterly, Associate Professor of Political Science at Iowa State University and defence analyst at ANSER, Inc. He has also been affiliated with research institutions including the East-West Center, The Brookings Institution, the Friedrich Ebert Foundation, and the Watson Institute for International Studies at Brown University among others. Dr Dombrowski is the author of over fifty books, monographs, articles, book chapters and government reports. Awards include a Chancellor's Scholarship for Prospective Leaders from the Alexander von Humboldt Foundation, the Navy Meritorious Civilian Service Medal, and the Navy Superior Civilian Service Medal. He received his B.A. from Williams College and an MA and PhD from the University of Maryland.

BIOGRAPHY OF SPEAKERS

Tobias Feakin

Tobias Feakin is the Director of the International Cyber Policy Centre, and Senior Analyst for National Security at ASPI. In this role he researches how cyber space is used for nefarious purposes at the state and sub-state level; creating collaborative policy responses; and creating national and international cooperation in cyber space. His previous work examined emerging vulnerabilities in critical national infrastructures, and developed into creating avenues for incorporating the private sector into cyber policymaking mechanisms, and examining how the exploitation of cyber space is leading to international geopolitical tensions. He was previously Director of National Security and Resilience at the Royal United Services Institute in London, and has also worked for the U.K. Government.

Tim Junio

Tim Junio is a cyber security fellow at Stanford University. He received his PhD in political science from the University of Pennsylvania in 2013. His dissertation focused on cyber warfare strategy, and how domestic politics -- particularly principal-agent problems between political leaders and national security bureaucracies responsible for cyber operations -- may increase the probability of escalatory responses to cyber attack. Dr Junio tested his theories with comparative fieldwork on how the United States, South Korea, and Taiwan produce and project cyber power. In his spare time, he develops new cyber capabilities at the Defence Advanced Research Projects Agency (DARPA). Before beginning his PhD studies, Dr Junio worked on cyber strategy and analysis for the Office of the Secretary of Defence, RAND Corporation, U.S. intelligence community, and Johns Hopkins' Information Security Institute.

Ram Levi

Ram Levi is a cyber security expert, founder and CEO at Konfidas Ltd. – a cyber security strategy solutions company. He is a Cyber Security adviser to the National Research and Development Council, Ministry of Science and Technology and Space. Levi is also a Senior researcher at the Yuval Ne'eman Workshop for Science, Technology and Security, Tel Aviv University. In 2011, he served as Secretary of the Prime Minister's National Cyber Initiative Task Force that spearheaded the government resolution on establishing the National Cyber Directorate. In 2010, he was a co-author of the President of Israel's committee on the Israeli National Space Policy, where he co-authored the national civilian space policy. Currently, Levi is running Konfidas, a cyber security company bringing a unique approach to prepare for cyber threats based on offensive attacker mind-set. Graduate of the International Space University (ISU), Levi holds a degree in Computer Science. He is a guest lecturer at: International Space University (ISU), Tel Aviv University, Technion – Israel Institute of Technology, The Interdisciplinary Center, Herzliya. Member of: the National Committee for Cybersecurity Research and Development, the Yuval Ne'eman Workshop for Science Technology and Security Senior Cybersecurity forum and IDC International Institute for Counter Terrorism Cyber Terror Group. Levi writes and gives lectures regularly on space and cyber security aspects.

John Lindsay

John R. Lindsay is a research scientist with the University of California Institute on Global Conflict and Cooperation (IGCC) and adjunct professor at the University of California, San Diego School of International Relations and Pacific Studies (IRPS). His research examines the impact of the information revolution on international security and has appeared in leading journals such as International Security, Security Studies, Journal of Strategic Studies, and Technology and Culture. Together with Professor Erik Gartzke at UCSD, he leads a new Department of Defence Minerva Initiative programme examining the impact of technological complexity on international strategy. He also teaches core courses in the Security of the Asia Pacific track of the IRPS Master of Advanced Studies in International Affairs programme. He holds a PhD in political science from the Massachusetts Institute of Technology, and an MS in computer science and BS in symbolic systems from Stanford University. He has served in the U.S. Navy, with assignments in Europe, Latin America, and the Middle East.

BIOGRAPHY OF SPEAKERS

Fabrice Marie

Fabrice Marie is a veteran of the old school hacking scene. Growing up coding and tinkering with 90's early systems, he absorbed the methodologies, ideas and technologies at large of the era, giving him a strong wide base in computing. Fabrice did his entire career in security at times on the attack front, others on the defence front, always coding, sometimes innovating interesting techniques and often accumulating eccentric online contacts in the scene. The past 10 years he has been focusing on securing APAC's large banks and telecoms. The last 2 years Fabrice has been busy heading the R&D department of Kibin Labs focusing on secure managed services and building a fully automated cloud and infrastructure management software with a very strong emphasis on security. Fabrice studied at Prytanée National Militaire de La Flèche, followed by the University of Caen. Originally from France, he is now a Singaporean citizen.

Mihoko Matsubara

Mihoko Matsubara is Cyber Security Analyst with Hitachi Systems, Ltd., Tokyo, focusing on geopolitical threats and policy issues. She is also Adjunct Fellow, Pacific Forum CSIS, Honolulu. Ms Matsubara previously served the Japanese Ministry of Defence for nine years, working with the U.S. government and military. Her contribution earned three letters of appreciation from the U.S. government. Upon graduation from the Johns Hopkins School of Advanced International Studies (SAIS), she worked at Pacific Forum CSIS as a resident fellow to research cyber security cooperation between Japan and the United States. Ms Matsubara is also active about publication and presentations or panel discussions. Her articles and papers have appeared in various outlets including Council on Foreign Relations' Asia Unbound and East Asia Forum. The RUSI Journal is publishing her latest piece regarding cooperation on cyber security between Japan and the U.K. soon. She was invited to multiple cyber security conferences and seminars to share her perspective at the AFCEA TechNet Asia Pacific 2013, Cityforum, and ISACA Tokyo Chapter. Ms Matsubara received her MA in International Relations and Economics from SAIS in Washington DC on Fulbright, and BA in Literature from the Waseda University, Tokyo.

Michael Raska

Michael Raska is a Research Fellow in the Military Transformations Programme at the S. Rajaratnam School of International Studies, Nanyang Technological University in Singapore. His research interests include East Asian security and defence, including theoretical and policy-oriented aspects of military innovation, force modernisation trajectories, information and cyber warfare. Dr Raska has taught at the Goh Keng Swee Command and Staff College (SAF Campaign and War Studies Course) and the Lee Kuan Yew School of Public Policy (International Security). His research experiences include visiting fellowships at the Hebrew University of Jerusalem, Yonsei University, Pacific Forum CSIS, and Samsung Economic Research Institute. He is an alumnus of the Columbia / Cornell University Summer Workshop on Analysis of Military Operations and Strategy (SWAMOS) and the Philip Merrill Center for Strategic Studies Workshop at Basin Harbor. He holds a BA in international studies from Missouri Southern State University (2000), an MA in international relations from Yonsei University (2002), and a PhD in public policy (2012) from the Lee Kuan Yew School of Public Policy, where he was a recipient of the NUS President's Graduate Fellowship.

Benjamin Schreer

Ben Schreer is Senior Analyst for defence strategy at the Australian Strategic Policy Institute (ASPI). Previously, Ben was the deputy head of the Strategic and Defence Studies Centre (SDSC) at the Australian National University (ANU) where he taught strategy at the graduate level, including in the Military Studies Programme at the Australian Command and Staff College (ACSC). Before coming to Australia, he held positions as the deputy director of the Aspen Institute in Berlin, leader of a research group at Konstanz University, and deputy head of research unit at the German Institute for International and Security Affairs (Stiftung Wissenschaft und Politik, SWP) in Berlin.

Doron Zimmermann

Since April 2012, Doron Zimmermann is Senior Manager Security Affairs at Swissgrid Ltd., Switzerland's national transmission system operator (power energy sector) and one of the country's most critical infrastructures. He manages government security relations, strategy development and is involved in security standards, critical infrastructure protection and security audits related projects. In his previous position, Dr Zimmermann served as senior staffer and head of section of the Swiss cabinet's inter-agency Security Committee Staff, where he was responsible for the integration of intelligence and headed a strategy development project mandated by the Swiss Federal Council through its Security Committee. He previously served as Assistant Professor of International Security Policy at the College of International Security Affairs (CISA) at National Defence University in Washington, D.C.; as Head of Political Risks at Soliswiss, Switzerland's oldest political risk insurer; and as Senior Researcher at the Center for Security Studies and Conflict Research, Swiss Federal Institute of Technology (ETH). He read for his PhD at the Faculty of History, Cambridge University (Emmanuel College), from 1994-1998.

RSIS PANEL CHAIRS

Richard Bitzinger

Richard A. Bitzinger is a Senior Fellow and Coordinator of the Military Transformations Programme at the S. Rajaratnam School of International Studies, where his work focuses on security and defence issues relating to the Asia Pacific region, including military modernisation and force transformation, regional defence industries and local armaments production, and weapons proliferation. Mr Bitzinger has written several monographs and book chapters, and his articles have appeared in such journals as International Security, Orbis, China Quarterly, and Survival. He is the author of Towards a Brave New Arms Industry? (Oxford University Press, 2003), Come the Revolution: Transforming the Asia-Pacific's Militaries, Naval War College Review (Fall 2005), Transforming the U.S. Military: Implications for the Asia-Pacific (ASPI, December 2006), and Military Modernization in the Asia-Pacific: Assessing New Capabilities, Asia's Rising Power (NBR, 2010). He is also the editor of The Modern Defense Industry: Political, Economic and Technological Issues (Praeger, 2009).

Caitríona Heinl

Prior to joining CENS, Caitríona Heinl was the lead researcher responsible for Justice and Home Affairs policy and the Justice Steering Committee at the Institute of International and European Affairs (IIEA), Ireland. Under this portfolio, she was required to conduct analysis on a wide variety of European and international issues such as European and international criminal justice, fundamental rights, data privacy and data protection, police and judicial cooperation, crime prevention and the fight against trans-national organised crime, counter-terrorism, international security and cyber-related issues.

Caitríona was the legal researcher and IIEA-based project manager for a study on behalf of the European Commission's Directorate-General Justice, Liberty and Security on non-legislative measures to prevent the distribution of violent radical content on the Internet including a transferability analysis of methods applied in the 27 EU Member States to prevent the dissemination of illegal content through the Internet. She was also a member of a European Parliament funded project, providing key information to Irish citizens on the work of the European Parliament. She holds a Masters (MPhil) in International Relations from the University of Cambridge.

Bernard Loo

Bernard F. W. Loo is Associate Professor and Coordinator of the Master of Science (Strategic Studies) degree programme at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University. He completed his doctoral studies at the Department of International Politics at the University of Wales, Aberystwyth in 2002.

He is the author of Medium Powers and Accidental Wars: A study in Conventional Strategic Stability (Edwin Mellen, 2005), and the editor of Military Transformation and Operations (Routledge, 2009). His other publications have appeared in the Journal of Strategic Studies, Contemporary Southeast Asia, NIDS Security Reports, and Taiwan Defense Affairs.

He is a regular commentator on defence matters, and his commentaries have appeared in The Straits Times (Singapore), The Nation (Thailand), and The New Straits Times (Malaysia). He has been invited to speak at a variety of defence-related institutions and conferences, in China, Estonia, Finland, Japan, New Zealand, and the Philippines. His research interests encompass war studies, strategic theory, conventional military strategies, strategic challenges of small and medium powers, and problems and prospects of military transformation.

Pascal Vennesson

Pascal Vennesson is Professor at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University and Associate Fellow at the European Union Centre in Singapore. He is on leave from the University Panthéon-Assas, Sorbonne University, Paris.

His research and teaching lie at the intersection of the fields of international relations and strategic studies. He is finishing a book entitled War in the Global Village: Transnational Challenges and the Struggle for Freedom of Action. He recently published "Sanctions and Embargoes in EU-Asia Relations" (with Clara Portela) in: T. Christiansen, E. Kirchner, P. Murray, eds., The Palgrave Handbook of EU-Asia Relations. Basingstoke: Palgrave, 2013. He is the author, co-author and editor of five books and his refereed articles have been notably published in Armed Forces and Society, International Relations, Journal of Strategic Studies, Review of International Studies, and Revue Française de Science Politique (French Political Science Review). He is a member of the editorial boards of Revue Française de Science Politique, and Security Studies.

PARTICIPANTS

Thomas Bondiguel
First Secretary (Political/Press)
French Embassy
Singapore

Liu Mun Kwong
Head, Cyber Defence Plans, JCSID
Ministry of Defence
Singapore

Ong Wei Chong
Assistant Professor
S. Rajaratnam School of International Studies (RSIS),
Nanyang Technological University
Singapore

Julian Snelder
Amiya Capital
Hong Kong

Tan Wei Chong
Branch Head
Ministry of Defence
Singapore

Gwendolyn Teong
Staff Officer
Ministry of Defence
Singapore

Paul Harris Wilt
Commander, United States Navy
Assistant Naval Attaché
Embassy of the United States of America
United States of America

Senol Yilmaz
Associate Research Fellow
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS),
Nanyang Technological University
Singapore

ABOUT RSIS

The S. Rajaratnam School of International Studies (RSIS) is a professional graduate school of international affairs at the Nanyang Technological University, Singapore. RSIS' mission is to develop a community of scholars and policy analysts at the forefront of security studies and international affairs. Its core functions are research, graduate education and networking. It produces cutting-edge research on Asia Pacific Security, Multilateralism and Regionalism, Conflict Studies, Non-Traditional Security, International Political Economy, and Country and Region Studies. RSIS' activities are aimed at assisting policymakers to develop comprehensive approaches to strategic thinking on issues related to security and stability in the Asia Pacific.

For more information about RSIS, please visit www.rsis.edu.sg

S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

A Graduate School of Nanyang Technological University

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