RSIS-TDSI SEMINAR 2016

Disruptive Defence Technologies in Military Operations

Event Report

29 June 2016

RSIS
Nanyang Technological University
S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

Event Report

RSIS-TDSI SEMINAR 2016

Disruptive Defence Technologies in Military Operations

Report of a seminar jointly organised by:
Institute of Defence and Strategic Studies,
S. Rajaratnam School of International Studies,
Nanyang Technological University,
and
Temasek Defence Systems Institute,
National University of Singapore

29 June 2016
Shaw Foundation Alumni House, National University of Singapore

TABLE OF CONTENTS

Workshop Administrators
Ben Ho Wan Beng and Wong Hsiao-Szu

Editor
Ben Ho Wan Beng

Rapporteurs
Henrik Paulsson and Eugene Mark Min Hui

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

This seminar adheres to a variation of the Chatham House Rule. Accordingly, beyond the paper presenters cited, no other attributions have been included in this event report.

EXECUTIVE SUMMARY

Throughout history, defence technology has profoundly shaped the character of war and warfare. The contemporary defence milieu is one marked by rapid developments, leading to a state of uncertainty for modern armed forces. Complicating matters is the advent of potentially disruptive technologies like unmanned systems and robotics, and the implications of these developments for the future battlespace would be profound. Against this backdrop, the RSIS-TDSI Seminar, which was held on 29 June 2016 at the National University of Singapore, provided a suitable platform for the assessment of the complex interplay between disruptive technologies and the military that operates them. Indeed, the seminar sought to bring RSIS and TDSI together to create an outlet for mutual learning as participants from both organisations can not only tap onto each other's expertise, but also discuss issues of mutual relevance.

To what extent would disruptive technologies shape the contemporary and future security environments? What would be the impact of technological innovations on militaries? To address these and similar key issues shaping the discourse, the seminar discussed the following themes: (i) the complex operating environment; (ii) disruptive defence technologies; and (iii) cyber issues. These three themes showed that technology and the strategic and cognitive decision-making in its use are underlying constants shaping the contemporary battlespace, and armed forces all over the world would do well to be adaptive in order to cope with this reality.

KEYNOTE ADDRESS

Mr Ng Chee Khern, Permanent Secretary (Defence Development) at Singapore's Ministry of Defence, began his keynote address by arguing that there is a need for Singapore to keep up-to-date with disruptive defence technologies. This would necessitate the Ministry of Defence working closely together with the academic community, and the inaugural RSIS-TDSI Seminar was an example of this nexus between the two entities. Mr Ng then provided a broad overview of the changes in military technology over the decades. Airpower was immensely disruptive, especially from World War Two onwards, as it revolutionised the operating environment. Prior to the introduction of airpower, land and naval forces fought largely in isolation. Airpower would change this state of affairs as it gave rise to new concepts such as joint operations. Since the Vietnam War, military technology has also developed apace. Disruptive systems such as precision-guided munitions (PGMs) were only available to the most advanced militaries some 20 years ago, but the diffusion of such technologies through globalisation means that small states also have access to them.

Mr Ng maintained that while the Singapore Armed Forces (SAF) has successfully incorporated such technologies, there is a need to strengthen the country's scientific and industrial bases to fully exploit these technologies. To be sure, the advent of PGMs has enabled better targeting, but they have also profoundly increased the importance of command, control, communication (C3), and intelligence, surveillance and reconnaissance (ISR) as the latter is the first component of the kill chain. That being said, the SAF has become a networked force with integrated command and communication nodes implemented force-wide. In closing, Mr Ng contended that we could be on the cusp of another Revolution in Military Affairs, with profound implications for the SAF. Disruptive technologies such as cyber-warfare capabilities and robotics could change the paradigm of warfighting. This is because cyber-warfare can disrupt operations in other domains of war, while robots are close to replicating the capabilities of human beings.

PANEL 1 | THE COMPLEX OPERATING ENVIRONMENT

COMPLEX ENVIRONMENTS

Dr Grant Hammond, a professor with the U.S. Air Force Center for Strategy and Technology, began his presentation by defining a complex environment as one with many, different, and rapidly shifting domains. So how do these complex environments change or influence military decision-making? The issue lies in how armed forces think. Military problem-solving has tended to be engineering-oriented and function within a three-dimensional spatial environment. This mentality is largely linear and concomitantly easy to visualise. Dr Hammond argued that the reality is different, though, with the environments being of a more non-linear and fluid nature. Events happening in these milieus are concurrent, intermittent, and along a four-dimensional temporal environment, and these factors make for a harder schematic representation. Complex environments can also have innumerable causes, are difficult, if not impossible, to define, describe, explain, or predict, and cannot be tackled by traditional problem-solving processes.

Dr Hammond argued that challenges profoundly shaping the world include the uneven distribution of wealth and resources, asymmetric demographic distribution, and the rising global reach of cyber-crime, cyber-espionage, and cyber-warfare. Developments such as the rise of non-state actors, large migrant flows, and climate change are compounded by technological developments like robotics and 3D printing. These challenges are upending established ways of thinking and managing issues. Traditional and conventional solutions are giving way to novel and multi-dimensional ones, while territorial significance is becoming temporal. The rapid acceleration of technological change has brought about a globally networked population, leading to an unprecedented global transparency. Summing up, Dr Hammond stressed that militaries and states need to adapt their decision-making and thought processes if they were to stay relevant in the complex operating environments of the contemporary strategic ecosystem.

WHY SMART DEFENCE TECHNOLOGY CAN MAKE US STRATEGICALLY STUPID

Dr Pascal Vennesson, a professor with the Military Studies Programme at IDSS, RSIS, started his speech by observing that many armed forces have adopted a heavily technological basis for modernisation, and that the SAF is one such military. The key implication is that smart defence technology can make commanders overly dependent on technology and this would impair their strategic decision-making. Building upon the research of the cognitive psychologist Gary Klein and part of a larger debate on command decision-making processes, Dr Vennesson used the cases of Generals Tommy Franks and Douglas MacArthur to show how technology can disrupt intuition and strategic decisions.

During the 2003 invasion of Iraq, General Franks utilised a “blue force” tracker – a screen that showed the exact location and status of U.S. units and their respective enemies. He saw that the map showed no Iraqi units close to the U.S. Army’s 5th Corps – yet the latter seemed to be not moving or fighting. General Franks was furious over this and complained to the force commander. In reality, one of the toughest battles of the war was unfolding, but this was not reflected on the tracker as American forces were fighting Iraqi units that were too small to be identified on the map. This is contrasted against the actions of General MacArthur, who after the North Korean invasion of the South in 1950, decided to travel to Seoul to assess the situation himself. The on-site perspective gave MacArthur the knowledge to make sense of the situation and adjust his plans accordingly.

Dr Vennesson added that the over-reliance on technology disrupts commanders’ pattern recognition, and reduces the users to becoming passive recipients of data. The latter is deemed essential or non-essential by pre-defined conditions and algorithms, functioning as a “black box” that denies the commander the ability to see the raw data and utilise the critical data elements in helping him reach his conclusions. Thus General MacArthur’s site visit served to give him the sense of the operation without relying solely on information provided by his subordinates. In contrast, General Franks did not have an accurate picture of how the metrics were collected, nor how the blue force tracker was functioning. In this light, relying too much on technology not only makes commanders less adaptive, but also distorts their mental models. Rounding up, Dr Vennesson stressed that when developing and adopting new technologies, militaries and designers must ask themselves if the technology is developed in ways that unintentionally compromise strategic expertise and intuition in commanders. How can it sustain and not dominate the commander’s strategic intuitions and safeguard his expertise? The more successfully these questions are answered, the more effective the military will be as a fighting force.

PANEL 2 | DISRUPTIVE DEFENCE TECHNOLOGIES

WILL TECHNOLOGICAL CONVERGENCE REVERSE GLOBALISATION?

Dr Thomas Hammes, a Distinguished Research Fellow with the Institute for National Strategic Studies in the U.S., framed his presentation to address the issue of how the diffusion of technology affects globalisation. Global trade and financial flows are both declining, and new technologies such as robotics and 3D manufacturing are largely behind this. Dr Hammes argued that these technologies reduce globalisation as they enable local producers to produce better, cheaper and more durable goods. As local production improves, more people would "buy local" rather than foreign goods. The upshot is the reduction in jobs, and the reinforcement of protectionism and isolationism. Indeed, the latter is on the rise recently as manifested in Brexit and developments of a similar nature.

Dr Hammes believed that Singapore is well-positioned for this manufacturing revolution, as it has a well-educated work force. This development would see Singapore reducing its dependence on foreign labour as new emerging technologies could improve productivity. The upshot is that Singaporeans' fear of foreigners jostling for jobs with them would be mitigated. Singapore's energy vulnerabilities could also be mitigated by renewable energy sources that are increasingly becoming available, such as solar and wind power. However, the city-state could also face reduced port traffic, as improved local production would reduce the demand for international shipping. Ditto a reduction in global financial flows. As Singapore depends significantly from port traffic and financial flows for its income, it would do well to monitor this development closely – that repetitive and routine jobs could also disappear means that Singapore needs to examine its business model and re-define its job market.

Rounding up, Dr Hammes discussed the implications of de-globalisation in the military sphere. The technological revolution allows small states to defend themselves more easily and at a lower cost. For instance, small states could acquire cheap drones in massive numbers. These drones can be easily hidden, for instance, in a shipping container. Any entity with access to such systems could then exploit this fact to carry out military missions such as drone strikes. As there are countless containers at any one time on the high seas, it would be a tall order for the party defending against the drone attack to find the drones in the first place. Thus, one could argue that defence has become dominant vis-a-vis offence.

THE BEAR AND THE DRAGON AGAINST THE EAGLE: MILITARY INNOVATION AND STRATEGIC THOUGHT IN RUSSIA, CHINA, AND THE U.S.

Dr Michael Raska, an assistant professor with the Military Transformations Programme at IDSS, RSIS, began his presentation with the question: "Why do great powers such as Russia, China and the U.S. respond differently to the same technological innovation?" He explained that the world is basically in a sixth wave of Revolution in Military Affairs (RMA) that is characterised by a new generation of precision weapons, advanced air defences, anti-ship weapons, cyber-warfare capabilities, space-launch capabilities and anti-space systems. Nevertheless, it is important to understand military innovation in the strategic contexts of Russia, China and the U.S. respectively. While U.S. has always been at the forefront of military innovation, Russia and China are catching up in terms of asymmetrical capabilities.

For the Russians, conceptual innovation is deemed more important than the technological one. Russia has a concept called the "New Generation Warfare", where it seeks to defeat the opponent using a combination of non-military and kinetic means. Indeed, warfighting using non-kinetic means such as information warfare has always occupied a central role in Russian strategic thought. Dr Raska next delineated the four domains the Chinese military are focusing on: (i) space; (ii) near-space; (iii) cyberspace; and (iv) underwater. Under the concept of "Near Seas Defence", China is emphasising these domains so as to offset American technological superiority. To this end, Beijing is investing heavily in missile, air, and naval power. Witness its introduction of the world's first anti-ship ballistic missile, the DF-21D.

In the face of these developments in its potential adversaries, the U.S. has not rested on its laurels. Indeed, Washington introduced the Third Offset Strategy last year that focuses on six areas: (i) anti-access and area-denial capabilities; (ii) guided munitions; (iii) undersea warfare; (iv) cyber/electronic warfare; (v) human-machine teaming; as well as (vi) war-gaming and concepts development. The idea is to exploit existing technologies against potential adversaries. For instance, there was a discussion in using swarming unmanned aerial vehicles (UAVs) to counter sophisticated enemy air defences. Some of these UAVs would deploy as decoys, while others would target the air defences, but both would work in tandem. Dr Raska concluded the presentation by stating that the world was currently in flux as strategy, operational art and technology are all developing apace.

PANEL 3 | CYBER ISSUES

CYBER-WARFARE SCHOOLS OF THOUGHT

Dr Paul Mitchell, the Director of Academics and Associate Dean of Arts at Canadian Forces College, began his talk by stating that the advent of cyber-warfare has presented us with a set of ontological and epistemological divides. The ontological point he made is that our existence is being redefined by technological changes. War has long been a clash of the moral forces of will, courage and risk. That said, industrialised warfare has introduced conditions that have gradually reduced the impact of such forces. Cyber is part of this form of warfare. It is not only an artificial domain that respects no physical boundaries, but a domain of endless, creative possibilities as well. This state of affairs has enabled new actors to challenge existing distributions of power and resources, and makes strategising difficult, especially for the defence. Thus, the epistemological question is: what could be done?

On that note, Dr Mitchell highlighted that there are currently three schools of thought on cyber warfare: (i) the conservatives; (ii) the revolutionary materialists; and (iii) the liberal materialists. The conservatives believe that the character of war changes over time, but not its nature. The nature of war is fundamentally violent and instrumental in purpose; however, cyber activities are often neither of those. Thus, if cyber-warfare is a factor in war, it is only an enabling one, but not a unique characteristic. Regardless, the conservatives argue that humans could still confront the complex challenges through their innate creativity and willpower. As for the revolutionaries, they argue that technology determines our reality. Cyber-warfare permits users to strike directly where their enemies are weak, obviating the need to target their strengths. Indeed, throughout history, there have been many examples where new technologies enabled the belligerent to skirt around exhausting combat in the field. Dr Mitchell postulated that cyber is the new high ground today. After all, one needs to dominate cyber-space before superiority could be attained in other domains. Revolutionaries also stress the loss of human agency in controlling events, and like airpower theorists, they view contemporary society as weak and unreliable.

As for the liberal school of thought, Dr Mitchell stated that this camp straddles both the conservative and revolutionary schools. Liberals acknowledge the technological changes confronting society, but maintain that humans determine how these technologies can be utilised. In other words, liberals not only echo the revolutionaries' view that society is changing not for the better, but also share the conservatives' belief in human agency. Nevertheless, liberals fear that the situation would get worse unless humans design their institutions to take into account new material conditions. Summing up, Dr Mitchell opined that no one school offers conclusive answers to the question of "What is to be done?" In fact, there is a widespread lack of agreement over the nature of cyber threats and the best approach in dealing with it.

REGIONAL SECURITY ARCHITECTURE IN ASIA: ENHANCING TRANSPARENCY AND CONFIDENCE AMONG MILITARIES ON CYBER

Ms Caitriona H. Heinl, a Research Fellow at the Centre of Excellence for National Security, RSIS, began her presentation by framing it into two sections: (i) approaches in regional security architecture vis-à-vis cyber that could complement each other; and (ii) finding common interests and identifying practical actions. Under the first section, Ms Heinl highlighted that there are four main approaches in regional security architecture that could complement each other. First, ongoing bilateral discussions and strategic dialogues on cyber issues could be extended to larger regional groups, and the defence community could be an important stakeholder in these dialogues. Traditional defence cooperative efforts could also include cyber matters. Second, there is a need to develop cooperation among like-minded entities within multilateral dialogues like at the Shangri-La Dialogue. Third, there is a need to further develop confidence-building measures and implement those already agreed upon. Lastly, existing institutional mechanisms are important to move ahead on practical cooperation. In May 2016, the 10th ASEAN Defence Ministers Meeting agreed to adopt the concept paper on ADMM-Plus Experts Working Group on cyber-security, and Ms Heinl argued that this is a useful step forward.

She then dealt with the issue of how to build a common understanding amongst militaries based on eight points. For one, there is a need for understanding how governments conceptualise cyber issues. Second, it is important to have conversations and increased levels of transparency in the region regarding this matter. Third, capacity-building could take place in non-sensitive areas, such as information sharing on best practice areas in how to attract and train both technical and policy experts for the defence community. Fourth, regular exchanges of defence officials and military-to-military linkages could include cyber issues. Fifth, the region could start with a focus on common challenges such as countering terrorist use of advanced cyber capabilities. Sixth, regional initiatives like the Network of ASEAN Defence and Security Institutions, the Council for Security Cooperation in the Asia Pacific, or the ASEAN Institute of Strategic and International Studies could examine subjects on cyber matters. Seventh, the ASEAN Regional Forum could explore practical cooperation for cyber capacity building or post-disaster reconstruction. Lastly, upcoming events could be leverage upon to enable cooperation. For instance, the Japan Olympics is being showcased for finding ways to build cooperation.

SEMINAR PROGRAMME

0830 – 0900hrs

Registration for speakers and participants

0900 – 0940hrs

Keynote Address
Mr Ng Chee Khern
Permanent Secretary (Defence Development), Ministry of Defence, Singapore

Chairperson
Mr Eddie Lim Meng Chong
Senior Fellow and Coordinator of the Military Studies Programme, IDSS, RSIS

0940 – 1055hrs

Panel 1: The Complex Operating Environment

Chairperson
Dr Bernard Loo Fook Weng
Associate Professor, Military Studies Programme, IDSS, RSIS

Complex Environments
Dr Grant T. Hammond
Professor, USAF Center for Strategy and Technology, Air University

Why Smart Defence Technology Can Make Us Strategically Stupid
Dr Pascal Vennesson
Professor, Military Studies Programme, IDSS, RSIS

1055 – 1115hrs

Coffee Break

1115 – 1230hrs

Panel 2: Disruptive Defence Technologies

Chairperson
Dr Ong Wei Chong
Assistant Professor, Military Studies Programme, IDSS, RSIS

Will Technological Convergence Reverse Globalisation?
Dr Thomas X. Hammes
Distinguished Research Fellow, Institute of National Strategic Studies, National Defense University

The Bear and the Dragon against the Eagle: Military Innovation and Strategic Thought in Russia, China, and the U.S.
Dr Michael Raska
Assistant Professor, Military Transformations Programme, IDSS, RSIS

1230 – 1330hrs **Lunch**

1330 – 1445hrs **Panel 3: Cyber Issues**

Chairperson
Dr Graham Ong-Webb
Research Fellow, Military Studies Programme, IDSS, RSIS

Cyber-Warfare Schools of Thought
Dr Paul T. Mitchell
Director of Academics and Associate Dean of Arts, Canadian Forces College

Regional Security Architecture in Asia: Enhancing Transparency and Confidence among Militaries on Cyber
Ms Caitriona H. Heinl
Research Fellow, Centre of Excellence for National Security, RSIS

1445 – 1505hrs **Coffee Break**

1505 – 1635hrs **Syndicated Group Discussion for TDSI students**

1635 – 1645hrs **Closing Remarks**
Mr Eddie Lim Meng Chong
Senior Fellow and Coordinator of the Military Studies Programme, IDSS, RSIS

LIST OF SPEAKERS AND CHAIRPERSONS

(In order of appearance)

SPEAKERS

Mr Ng Chee Khern || Permanent Secretary (Defence Development)
Ministry of Defence
Singapore

Dr Grant T. Hammond || Professor
U.S. Air Force Center for Strategy and Technology
Air University
The United States of America

Dr Pascal Vennesson || Professor
Military Studies Programme
S. Rajaratnam School of International Studies
Nanyang Technological University
Singapore

Dr Thomas X. Hammes || Distinguished Research Fellow
Institute of National Strategic Studies
National Defense University
The United States of America

Dr Michael Raska || Assistant Professor
Military Transformations Programme
S. Rajaratnam School of International Studies
Nanyang Technological University
Singapore

Dr Paul T. Mitchell || Director of Academics and Associate Dean of Arts
Canadian Forces College
Canada

Ms Caitriona H. Heinl || Research Fellow
Centre of Excellence for National Security
S. Rajaratnam School of International Studies
Nanyang Technological University
Singapore

CHAIRPERSONS

Mr Eddie Lim Meng Chong || Senior Fellow and Coordinator of the Military Studies Programme
S. Rajaratnam School of International Studies
Nanyang Technological University
Singapore

Dr Bernard Loo Fook Weng || Associate Professor
Military Studies Programme
S. Rajaratnam School of International Studies
Nanyang Technological University
Singapore

Dr Ong Wei Chong || Assistant Professor
Military Studies Programme
S. Rajaratnam School of International Studies
Nanyang Technological University
Singapore

Dr Graham Ong-Webb || Research Fellow
Military Studies Programme
S. Rajaratnam School of International Studies
Nanyang Technological University
Singapore

ABOUT THE S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

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

For more information, visit www.rsis.edu.sg

ABOUT THE TEMASEK DEFENCE SYSTEMS INSTITUTE

Temasek Defence Systems Institute (TDSI) is a strategic alliance between two eminent institutions: the National University of Singapore and the US Naval Postgraduate School. TDSI was established on 11 July 2001 to provide the platform to bring together military staff and defence technologists in an education and research environment. TDSI aims to produce graduates who understand the complexities of a military force, so as to be able to create maximum leverage by the integration of operations and technology.

For more information, visit www.nus.edu.sg/tdsi

RSiS
Nanyang Technological University
S. RAJARATNAM
SCHOOL OF
INTERNATIONAL
STUDIES

Nanyang Technological University
Block S4, Level B4, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg