INTERNATIONAL CONFERENCE ON EMERGING AND DISRUPTIVE TECHNOLOGIES (ICEDT)

13–15 SEPTEMBER 2009
SINGAPORE

PONDER THE IMPROBABLE

NATIONAL SECURITY COORDINATION SECRETARIAT

INTERNATIONAL CONFERENCE ON EMERGING AND DISRUPTIVE TECHNOLOGIES (ICEDT)

REPORT ON THE WORKSHOP JOINTLY ORGANIZED 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)

13 – 15 SEPTEMBER 2009
SINGAPORE

CENTRE OF EXCELLENCE FOR NATIONAL SECURITY
S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
NANYANG TECHNOLOGICAL UNIVERSITY
2009

Contents Page

Rapporteurs: Clinton Lorimore, Gregory Dalziel, Jenna Park, Ng Sue Chia, Yeap Su Yin, Yolanda Chin

Edited by: Jenna Park, Gregory Dalziel

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

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

Executive Summary

The International Conference on Emerging and Disruptive Technologies (ICEDT), jointly organized by the Centre of Excellence for National Security (CENS), Global Futures Forum (GFF) and the National Security Coordination Secretariat (NSCS), was held at the Marina Mandarin Hotel, Singapore from 14 to 15 September 2009. ICEDT was a two-day conference jointly organized by CENS, GFF and NSCS, following last year's conference titled "Radicalization: Foresight and Warning."

The impact of science and technology on national security has become increasingly evident in recent years. Such impact is particularly acute in the field of terrorism and counter-terrorism. Recent attacks clearly demonstrate that terrorists are highly adept at using the latest technology to carry out their intentions. However, it is fair to state that policymakers in charge of national security seldom possess deep knowledge and expertise in the fields of science and technology. Conversely, scientists and technologists are often not well-versed and informed about national security policies as well. Accordingly, ICEDT was organized in recognition of this, and experts engaged in the field of science, technology and national security from the United States, Canada, Japan, Australia and the Asia Pacific were gathered to share their expertise, ideas, knowledge and experiences.

ICEDT was divided into four panels with syndicate group discussion to facilitate discussions based on the issues covered throughout the conference. The first panel, "Globalization and Innovation", touched on how globalization has contributed to growth in the trans-national dispersion of technological and scientific information, hence facilitating the rise of innovation. The next two panels were on "Dual Technologies and ICT." The first dealt with scientific and technological issues, and professional scientists and technologists delivered presentations related to their specific expertise; while the latter panel focused on the relationship between technology and national security, and explored issues such as the adaptation of Information Technology (IT) by terrorists as well as examining technology from a Revolution in Military Affairs (RMA) perspective. The last panel, "Other Technologies and Wild Cards," attempted to "scan the technological horizon" and address the reproductive, multi-utilitarian characteristic of disruptive and emerging technologies and the possible threats that these may pose to national and global security in the future.

The conference ended with the syndicate group discussions, and implications drawn from each group were presented for further discussion at the closing panel. Key implications derived from this conference were that governments should always be aware of the technological trend to "keep ahead of the game" and identify potential threats and dangers; scientists and technologists should be able to work integratively with policymakers and openly communicate with each other; and that states must cooperate together and share ideas and information. All in all, the integration of people and institutions with different expertise was identified as the key factor to prevent "technological surprises" by adversaries.

Welcome Remarks by Ambassador Barry Desker

Ambassador Barry Desker, Dean of the S. Rajaratnam School of International Studies (RSIS), began his Welcome Remarks by warmly greeting the guests and participants of the International Conference on Emerging and Disruptive Technologies. Ambassador Desker stated that the objective of this collaboration between CENS, GFF and NSCS was to create a multinational community of stakeholders of homeland security engaged in the collective analysis of global security issues.

ICEDT was the second conference jointly organized by CENS, GFF and NSCS, which followed the conference last year titled "Radicalization: Foresight and Warning". Ambassador Desker recalled that last year's focus was on the human dimension, exploring the recent violent manifestations of religious radicalization in the Southeast Asian region, while this year's focus shifted to the technological dimension. Noting how the world continues to be shaped by technology and its evolving manifestations, Ambassador Desker opined that technology was like a double-edged sword, which carried potential dangers along with its convenience and efficiency. The recent Jemaah Islamiyah (JI) improvised backpack IED attacks on the JW Marriott and Ritz-Carlton hotels in Jakarta clearly demonstrates that terrorists are clearly adaptable in exploiting technology to achieve their malicious purposes.

Therefore, it is crucial for national security practitioners to start paying attention to the technological aspect of national security and to address the threats and potential dangers posed by emerging and disruptive technologies.

In this regard, Ambassador Desker stated that the aim of ICEDT is to gather specialists from the hard and social sciences, as well as policy practitioners from different government sectors into one place, providing them with an opportunity to exchange their views. The participants of this conference were encouraged to discuss the issue of how adversaries (state or non-state) could exploit emerging technologies such as nanotechnology and biotechnology — as well as dual-use innovations — to pursue their malicious intentions and thus endanger societies. Ambassador Desker added that it was also important for the participants to identify possible domestic and international policy initiatives that could prevent and mitigate the dangers of the exploitation of technology by terrorists.

After encouraging the participants to share their expertise and perspectives, Ambassador Desker concluded that ICEDT would provide a useful framework to discuss and deepen our understanding of the critical relationship between technology and national security.

Ambassador Barry Desker delivering his Welcome Remarks.

Welcome Remarks by Susan H. Nelson

Susan Nelson, Director of the Office of Outreach in the Bureau of Intelligence and Research (INR/OTR), spoke on behalf of the U.S. Department of State and extended her welcome to the participants and speakers of the conference. She thanked CENS and NSCS for taking part in organizing the conference, which would launch an ongoing dialogue on emerging and disruptive technologies.

Ms. Nelson began by providing a brief explanation of the role of the U.S. Department of State and the mission of the Office of Outreach in the Bureau of Intelligence. The U.S. Department of State is in charge of managing U.S. relations with all countries on all issues all the time. The role of the Office of Outreach is to support the State Department by bringing together expertise inside and outside the government. This is to facilitate deep discussions in broad areas that would bridge the respective fields of technology and national security, thus enabling policymakers not to be caught off-guard by "disruptive" surprises arising from technology.

Due to globalization, it has become difficult for the government to single-handedly tackle domestic and international challenges in a fast-paced world. Therefore, it is crucial for the government to reach out to experts outside government and around the world. Ms. Nelson stated three reasons for this: (i) the exchange of information; (ii) the sharing of ideas; and (iii) the generation of new insights. Through gathering experts engaged in diverse fields, the U.S. government seeks to gather a diversity of perspectives and employ them into the analytic process to tackle diverse challenges. The role of GFF is to foster such collaboration and bring together information and perspectives in diverse fields in the international community. Ms. Nelson stated that she hoped ICEDT would create new interests in areas where both technology and national security converge. She reminded the participants that throughout the conference, they should constantly keep the following questions in mind: (i) how can technologies surprise us; (ii) how can they be used differently; and (iii) how will they change the world?

Ms. Nelson stated three main goals of this conference:

1. Foster proactive dialogues and interaction with policymakers in the government.

2. Enhance understanding of emergent technical issues, threats and opportunities.

3. Anticipate and shape the future.

The speakers and participants each had specific expertise, and through this conference, it was hoped that they would be able to weave the presentations and discussions together to analyze and look at the big picture of the future.

Ms. Nelson added that, most importantly, the conclusions and implications drawn from this conference must necessarily be relevant to policymakers and help them make good decisions.

Susan Nelson delivering her Welcome Remarks on behalf of the U.S. Department of State.

Opening Address by Professor Lui Pao Chuen

In his opening address, **Professor Lui Pao Chuen**, Chief Scientific Advisor of the Ministry of Foreign Affairs, gave a detailed introduction of Singapore and its national defense infrastructure.

A small country once famously referred to as a red dot on the map, national defense has naturally become one of the most crucial issues for Singapore. In order to "survive and thrive" and overcome outside pressures, Professor Lui opined that Singapore had developed three attributes:

1. Agility: Singapore must act swiftly when it comes to decision and implementation, and change course when it takes a wrong direction.

2. Integration: Singapore must be able to integrate people within organizations, motivate collective action between different organizations and constantly look back to the past to make new decisions.

3. Openness: Singapore must be open to new ideas, talent and investment from outside.

In order to achieve happiness, prosperity and progress in Singapore, Professor Lui identified several inter-dependent elements. First of all, the nation has to have confidence in itself, and confidence comes from a good government providing stability. This sense of stability is provided by strong national security and, therefore, it is important for Singapore to focus on national security to ensure a stable society that is resilient to external and internal pressures. Because of this, Singapore has focused on identifying its hazards and has constantly worked on reducing and mitigating these hazards over time.

Professor Lui pointed out that there must be an open flow of information between intelligence and operations. The Singapore government realized the necessity of the integration between intelligence and operations and established the National Security Coordination Secretariat (NSCS) as a coordinating body between all ministries. In addition, the government has gone further to include educational institutions such as RSIS in this integration.

Recently, Singapore has begun integrating technology into its effort to stabilize its national security. Through the use of technology, Singapore seeks to surprise its enemies and prevent itself from being surprised by its enemies. This is evident in the speech delivered by former Deputy Prime Minister and Minister for Defence Dr. Tony Tan in 2000. In his keynote address, Dr. Tan stated that a strong capability in defense technology was critical to ensure national security and stressed the importance of gathering engineering and scientific talent in order to form the nucleus of Singapore's engineering and R&D efforts. Professor Lui himself foresaw that technology would become more and more important, as wars in the future would be more integrated featuring: (i) multiple source targeting; (ii) attack with multiple missiles; and (iii) continuous coverage.

In the course of his opening address, Professor Lui presented Singapore as an example of a country that had not only invested a lot of resources in national defense, but had also sought to merge intelligence and operations together, keeping its national defense system updated through technology. He concluded his opening remarks by stressing the importance of integration to ensure national security, and hence provide security and safety to society.

Professor Lui Pao Chuen introducing the Singapore national security system for his Opening Address.

KEYNOTE PRESENTATION

Avoiding Technological Surprises: Measures and Countermeasures

Ruth David spoke on the influence that globalization has on scientific discovery and innovation, and the measures or countermeasures needed to avoid technological surprises. David remarked that the ability to imagine the possible uses or abuses of technological applications is as important as efforts made to anticipate scientific discoveries or to forecast the maturation of emerging technologies. She also added that the changes, accelerations and impediments to scientific and technological innovations could be studied through the way that technology is currently used by security enterprises.

The connections or dialectical influences between information and people could be broadly understood in four key phases. David described the first phase (1990–2000) as the "People-to-Information" stage, wherein research could be done worldwide with information readily available at the end-users' "fingertips." In the second phase (2000–2010), technological or web advances have been able to connect people of similar research scopes and interests via social network platforms, hence connecting people to people. She termed this the "People-to-People" stage.

David remarked that we are now moving towards the third stage (2010–2020), termed the "Information-to-Information" age, where web-users would ideally be able to yield new insights from semantic web applications that could link related information from different databases together. The fourth phase (2020–2030) in web-based developments would be, in David's opinion, characterized by applications that could link "People-to-Knowledge." This represents a stage where web-based technologies could be accessed for meaningful answers to multi-disciplinary questions. This also suggests a possible move towards "intelligent web" innovations.

As for the influence of globalization on research alliances, David commented that this could be seen in the form of: (i) Institution-to-Institution; (ii) Department-to-Department (Discipline Based); or (iii) Peer-to-Peer (Individual Researcher Level) collaborations. She also added that the merging of academic and industrial research represented a departure from traditional entrepreneurial-opportunity to "problem focused, creative and strategic" research efforts. Seoul's Digital Media City and Singapore's Biopolis are examples of

strategic collaborations driven by academia, industry, and the state; where resources and even visions are pooled and shared to foster the development and testing of specific informational, technological and biological models. This also attests to the shift from companies being the core innovators to countries creating the right environment for innovations and tapping into the wisdoms of the crowds.

David opined that there was no single solution to avoiding technological surprises. Instead, its emergence could be anticipated or countered by not only contemplating what kind of technology could possibly emerge, but also imagining the ways that technology could be used. Given the global footprint of scientific and technological developments and the rate or pace at which, for instance, information technology changes, it might prove challenging to avoid technological surprises altogether. It was also suggested that an analytic cycle of "analysis-synthesis-inquiry" could be followed to map out all possible uses of technological breakthroughs. In this model, a series of roadmaps, scenarios and even games are considered to make sense of science and technology (S&T) enterprises and innovations. All in all, David concluded, efforts to anticipate the impact of technological advances must be as global, collaborative and dynamic as the S&T enterprises themselves.

Discussion

In response to questions on the practicality and objectives of building research parks, a speaker remarked that such developments often stood a better chance at the bridging of markets to research requirements and needs. The research parks in China are cases in point that the recognition of a country's market potential, size and capabilities helped favor the growth of innovation and that of the science community. It was also highlighted that cultural factors, more specifically existing research and risk-taking cultures, could either promote or impede innovations and the creation of new technologies.

Ruth David sharing her thoughts about possible measures and countermeasures to avoid technological surprises.

PANEL 1:

Innovation and Globalization

Disruptive Technologies: Redefined

George Atkinson explored in his presentation the consequences of disruptive technologies from a security and policy perspective. In particular, Atkinson focused on global events that are increasingly shaping the way S&T advances are assessed. The three primary issues affecting S&T strategies at the outset of the twenty-first century were: (i) the increasing competition among international co-operations pursuing emerging and "at-the-horizon" S&T; (ii) a rapidly expanding and aging population; and (iii) the social and ethical changes that S&T developments might bring forth.

A government's ability to foster safe and prosperous "knowledge-based" societies rests on how well government policies are able to recognize the opportunities and risks associated with emerging and "at-the-horizon" S&T, as well as to balance short- and long-term needs. Atkinson added that predicting the exact disruptive potential of resultant scientific achievements was difficult and required an understanding of current realities or global events that might cause significant societal change. For one, the typology of science contributors is changing and "internationalizing." There has been a vast increase in scientific contribution from states or individuals beyond the boundary of the United States. In this light, Atkinson mentioned that S&T might, among other things, promote access to information and knowledge (citizen empowerment), promote transparency through open publication and promote mutual respect for diverse views.

Atkinson stressed that for a more sophisticated understanding of the most recent S&T advances, it was important to expand the definition of "disruptive technologies" to include global and disruptive events.

Infectious diseases, for instance, are a leading cause of human suffering and pose a major threat to international commerce. However, what we lack is the coverage, especially by the media, of the roles and complexity of S&T factors required to effectively combat infectious diseases, and their impact on both domestic and international health policies.

Atkinson also added that the rapidly rising world population would exacerbate issues related to human health and this would also include food security and energy-related concerns. Essentially, current realities would shape the way S&T advances and is assessed. To this end, Atkinson urged for a strategic analysis of S&T developments. In this approach, realistic net assessments are obtained for the balancing of resources needed to address urgent security issues with those required for the patient and anticipatory analysis of emerging global S&T.

Lastly, Atkinson spoke on the role of the Institute of Science for Global Policy and how the institute has sought to assist governments to formulate and implement S&T policies to guide their investments in financial and human resources. More pertinently, he highlighted the importance of the need to bridge the gap between the science and policy communities through critical debates so as to achieve an accurate understanding of S&T options. The way forward would not just require an acknowledgement of the limitations of science and that of policymakers, but also a broadened definition of disruptive technologies.

George Atkinson delivering his presentation about disruptive technologies from a security and policy perspective.

Emerging Technologies: Sustainable Development & Stability

Richard Silberglitt presented on the possible linkages or connections between emerging technologies, sustainable development and security. His hypothesis is that emerging technologies can help economies grow and reduce conflict. He opined that broad-based economic development that creates jobs and improves the quality of life could remove the seeds of conflict. The roadmap to achieving economic development and stability would require the identification of technologies based on forward estimation of a country's local capacity.

According to Silberglitt, technology could play a pivotal role in enforcing institution-building mechanisms, especially in key "post-conflict priorities" like providing security, humanitarian relief and governance. In fact, a recent RAND study identified several emerging technologies that are highly likely to create a social impact by 2020. These include: (i) cheap solar energy; (ii) rural wireless communications; and (iii) ubiquitous information access. Silberglitt added that the results of this study were in line with Freeman Dyson's claim that emerging technologies have the potential to promote social justice in the twenty-first century. However, a caveat was added that, to sustain the conditions needed for economic development, technological solutions have to be considered and applied with local capacities, needs and barriers in mind (e.g. literacy level and availability of financial resources).

In light of this, Silberglitt mentioned that technology foresight, as a planning and policy tool, could be applied to explore the plausible future technology developments or applications that are better suited for a country's development needs and constraints. For instance, technology foresight could be applied to anticipate the sets of prevention (e.g. medicine and computer-assisted drug development), surveillance, and detection (e.g. bio-nano diagnostic and networked biosensors) measures required to combat the spread of emerging infectious diseases.

Silberglitt discussed a RAND study commissioned by Tianjin Binhai New Area (TBNA) and Tianjin Economic Technological Development Area (TEDA) in northeast China to study ways in which they could achieve economic growth through technological innovation. The results of the study bear testimony in how technology foresight can be used as a tool to identify key technology applications. Essentially, a key learning from the project is that sustainable implementation of technological solutions or applications depend on how well local constraints and drivers could be addressed and tapped on respectively. It was also added that building of local capacities, as in the case of developing countries, would also require a fair degree of international assistance or collaboration.

In closing, Silberglitt stressed that while certain technology applications would contribute to the creation of a "chaotic world" (e.g. support the proliferation of weapons of mass destruction and impede global information network security), emerging technologies could still be harnessed for constructive purposes. In particular, RAND envisions a linked world where international cooperation forms the basis of a preferred roadmap to the attainment of such ideals as country stability and economic power. Silberglitt thus re-emphasized the importance of technology foresight in helping countries identify and implement emerging technologies that could sustain economic growth.

Richard Silberglitt presenting on how emerging technologies can be used for sustainable development and stability.

Discussion

A participant queried if it would be possible to determine which technologies or applications are applicable to the economic development needs of individual countries. A speaker replied that the technological solutions and applications chosen or identified should vary according to local conditions (e.g. budget, literacy level) and individual community's needs. It was then asked if culture had an influence on science. A participant opined that the way information was interpreted and the meanings attached to data suggested that science-related problems could be a product of cultural mediation. A speaker responded that the science community had probably failed to effectively communicate scientific contributions to the policy community. Perhaps, it reflects a lack of time and interest in the policy community. It was stressed that both communities must "move together" and be willing to ask the right questions. A participant sought further clarification on the degree of influence that, for example, the arts had on and should be incorporated into our prediction of the future. Additionally, how we think about technologies and their applications could well be shaped by cultural elements. The arts community would probably be able to imagine or anticipate technological change and provide fresh insights. The speaker responded that questions on science, science fiction and the contributions of the artistic communities highlight, rather, the challenge of establishing a "timeframe" for innovation advances and change. This is to say that difficulty exists in determining what technological development is plausible or feasible within a given time span.

PANEL 2:

Dual Technologies and ICT (I)

Nanotechnology, Ecosystems and Urban Infrastructure

Terry Turney spoke on the issue of emerging technologies using a systems point of view. He began his talk by explaining that nanotechnology is not a technology, but rather a tool kit for working at a particular length-scale. He emphasized that we could not think about nanotechnology as a discrete entity, but as a mixture of chemistry, physics, engineering and biology. The excitement surrounding nanotechnology stems from the fact that we are now able to manipulate matter at a much smaller length-scale than was possible before. He went on to state that while we were just beginning to understand how to do this, nature had been doing this successfully for 3.5 billion years. Turney went on to argue that if we wanted to know how to develop nanotechnology properly, we need to examine how nature had engaged in nanotechnology. He went on to explain that while we could take inspiration from nature, we still had an advantage over nature in that we did not have to play by its same rules.

Turney explained that nanotechnology enables us to modify materials' properties. Modifying materials' properties enables extended product life times, better performance from those materials and allows for cost reductions. By utilizing nanotechnology, we can now begin to look at embedding feedback loops into the materials so that they become almost self-aware. There are also applications for nanotechnology in the area of energy generation, so that we can forget about the traditional methods of energy production such as coal, gas and nuclear sources; and instead look to where we can scavenge energy from vibrations and pressure differences. By using nanotechnology, we are able to change the way we use energy, how we supply society and how we use our food. Nanotechnology is also having an impact on business models, where businesses are going to begin providing a service rather than a product, through the selling of knowledge. Turney explained that this is an ongoing process that is becoming more ubiquitous.

While there are many benefits that can be gained from utilizing nanotechnology, Turney also pointed out that there are a number of possible dual-use purposes in which nanotechnology could be used for ill purposes. Some of these threats include the use of cryptic epitopes, where someone can design folding proteins that might appear to the body to be a foreign object and trigger an allergic response. Turney also explained that nanotechnology could be used for counterfeiting quite effectively. However, he explained that while there are possible threats associated with nanotechnology, the benefits far outweigh the possible threats to security. Turney finished his talk by stating that his view of how to approach nanotechnology was best exemplified by Leonardo Da Vinci's argument: "Those who are inspired by a model other than Nature, a mistress above all masters, are laboring in vain."

Terry Turney explaining how nanotechnology can be used to improve our lives.

Bio-nanotechnology and Security: Is Small Scary?

Margaret Kosal spoke on the issues of bio-nanotechnology and security. She began the talk by presenting a number of security puzzles. The first question she asked was whether nanotechnology had unique strategic value. She explained that the question remained unanswered because we had not seen the long-term effects of nanotechnology. Kosal then went on to ask how academics could make the issues surrounding nanotechnology relevant to policymakers so that these important issues might be addressed. She opined that we need to go beyond the "hope" and "horror" hype associated with nanotechnology.

Kosal gave a brief overview of literature concerning the nefarious uses of nanotechnology and argued that much of the work out there seemed to enter into the realm of science fiction, particularly when scenarios of "Grey goo" were discussed. She argued that this was impossible as it

had issues with the Second Law of Thermodynamics. In an effort to move beyond the science-fiction scenarios found in some literature, Kosal suggested a number of technically robust scenarios in which she examined how one might overcome counter-measures that had been developed. She then explained that there was research being done to target cancer cells with nanotechnology, but that this same kind of research could entail developing a way to overcome the anthrax vaccine by creating a toxin that could not be detected by current counter-measures. She stated that such a scenario was derived from research in academic journals and was based on a robust science and engineering foundation.

Key security factors associated with nanotechnology include the issues of deniability and a lack of transparency, as well as dual-use concerns, in which biotechnologies are potentially applicable to malfeasant co-option. There is also a caveat that biological agents require damp environments with moderate temperatures, moderate pressures and ambient oxygen, and the fact that nano-engineered materials do not replicate. Kosal also suggested that the lack of explicit norms associated with nanotechnology, specifically in the area of international arms control regimes, needed to be improved. She then cited the fact that, because there was no single discipline on which to focus, this made the task all the more complicated. Kosal stated that she believed the threats — if they were to arise — would come as a result of state-based proliferation. She also questioned whether there might be a rogue scientist scenario where an "AQ Khan of nanotechnology" might appear.

Margaret Kosal sharing her thoughts about the connection between bio-nanotechnology and national security.

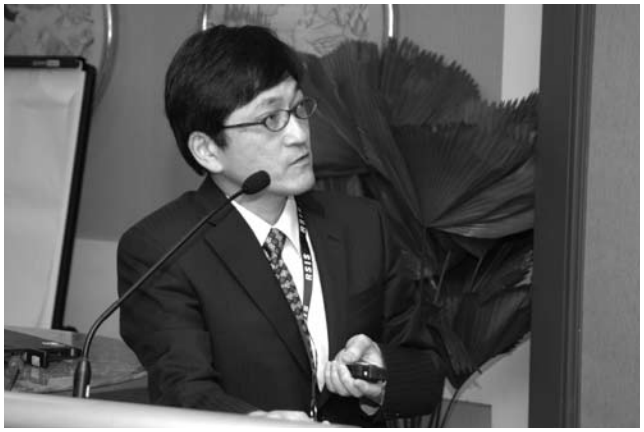
Dual-use Issues and Education for Life Scientists

Nariyoshi Shinomiya began his talk by citing a newspaper article titled "Scientist's honor and destroyer's dishonor," which addressed the question of which scientist did the most damage to the earth. The winner of the "contest" was U.S. scientist James Conant (1893–1978), who took the initiative to produce poisonous gases in World War I. The article also mentioned the "runner up," another U.S. chemist, Thomas Midgley (1889–1944), who invented leaded gasoline to suppress car knocking. Midgley also succeeded in synthesizing dichlorodifluoromethane (CFC), which serves as the cooling media of refrigerators and air conditioners, abstergent of electronics, and gas for sprays. Midgley's work has helped to increase air pollution and has aided in the destruction of the ozone layer.

With these two men in mind, Shinomiya asked to what extent scientists should take responsibility for their discoveries and inventions. He explained that the starting point of the problem is that while life scientists want to produce good research and contribute to social welfare and health, they could not exclude the possibility of the malign use of their research results. An example of dual-use research cited by Shinomiya was the scientist Fritz Haber (1868–1934), who won the Nobel Prize in 1918 for the development of a process for synthesizing ammonia, a process that has been important for the development of fertilizers. However, Haber subsequently became known as the "Father of Chemical Warfare" because of the dual-use nature of his innovation.

Shinomiya noted that there are concerns surrounding the "weaponization" of viruses by terrorists. He suggested that, beyond terrorism, a pandemic might be spread by careless scientists. However, he attempted to quell fears associated with biotechnology by stating that, for the most part, it was not an urgent problem. However, in order to get in front of the problem, Shinomiya suggested that, to overcome some of the issues associated with the dual-use dilemma, governments implement national guidelines for oversight of dual-use research at both the local and federal levels.

He also recommended that programs for bio-security education and training for all scientists and laboratory workers at federally funded institutions be implemented, focusing on the development of a code of conduct for scientists and laboratory workers in life sciences research. Shinomiya suggested that there also needs to be strategies that move beyond just the country level and that there be coordinated international oversight of dual-use research. He concluded by saying that there are many bioethics modules and education opportunities that need to be explored, and that bioethics could be a good starting point to develop dual-use education for life scientists.



Nariyoshi Shinomiya suggesting possible ways to educate life scientists on dual-use issues.

Evolving Tactics — Exploiting Advances in Simulation and Machine Learning Technologies

How Khee Yin began by describing how the choice of the right set of tactics is a function of experiences — both negative and positive. From there, he presented the implications that simulation and machine learning technologies have had on national security.

He explained that in an experiment he conducted, a team of robotic computers-generated learning entities were let loose in an indoor simulation environment where they were guided by a rule base of randomly generated rules to search and destroy targets. The rule base learned was implemented successfully on a real robotic platform and tested in a real-world environment. The learned rule base from the simulation managed to control a team of simple robots to accomplish the search-and-destroy task in the real world. This demonstrated the potential of first learning tactics in the simulation world before transferring for execution in the real world.

How provided another example of simulation and machine learning technologies by sharing an experiment involving a First-Person Shooter Game that played against other computer-generated entities and human players. As it played, the learning computer-generated entity dynamically adjusted its action selection rules based on the evaluation criteria of the competition, which was to exhibit human-like behaviour as determined by a panel of judges who were players themselves. The learning computer-generated entity did reasonably well in the competition in terms of humanness rating. He explained that the learning computer-generated entity had managed to learn rules during its run time while in the game mode.

How explained that with learning computer-generated entity technology, it would be possible to imagine a use where a human player could improve his tactics while playing against a computer-generated opponent. An opponent that adapts and learns in computer games would afford the human user a realistic environment to rehearse his tactics prior to execution, ensuring a higher chance of execution success in the real world. How also went on to argue that the simulation world is a safe place for individuals or groups to experiment and explore their ideas, fantasies and tactics. It is also a world where individuals or groups from different places can meet, facilitated by the Internet backbone — witness the growing popularity of a simulation world like Second Life. Another simulation the speaker suspected would continue to grow were networked game environments, the likes of massive multi-player online games, attracting multiple players from different parts of the world facilitated by the Internet. He concluded by stating that the future simulation world, together with easy access enabled by the Internet and learning computer-generated entities, are emerging technological areas to watch.

How Khee Yin demonstrating how simulation and machine learning technologies can be used to improve tactics and strategies.

Discussion

One of the participants asked about the accessibility of technologies to individuals with nefarious intent. The speakers seemed to be in agreement that the use of new and emerging technologies discussed is accessible to those with the necessary technical skills. One speaker stated that, in terms of accessibility, we were not in a position to put the genie back in the bottle, but we must now work on the control side of the equation. Another speaker suggested that access varies across different technologies, and that there are multiple barriers, such as gaining access into the laboratory area. The speaker added that there was a need for engineers to really turn the technologies discussed into effective weapons. This statement prompted an audience participant to argue that there were a lot of easier ways to kill lots of people than by adopting many of the possible scenarios suggested by the speakers. The participant then went on to argue that we need to move beyond the possibilities of what could happen and instead focus on what is likely to happen when examining new and emerging technologies.

PANEL 3:

Dual Technologies and ICT (II)

Terrorist Use of Information Technology and Implications for Counter-Terrorism Policies

In his talk, **Alexander Lim** examined the use of information and communication technologies by terrorist organizations and discussed the implications for counter-terrorism policies.

The Internet has dramatically changed the mode of interaction between terrorists, enabling them to move from largely face-to-face interactions to virtual meetings using the Internet, in turn changing the profile of terrorists. Before 2004, Lim explained, the average age of a terrorist was 26, with membership in terrorist groups largely formalized. However, since 2004, Interpol has noted that the average age has dropped to 20 years, with more women involved and there being what Interpol described as "part-time cyberterrorists." Lim explained that the Internet offers a number of things that may explain this change. These include: (i) easy access; (ii) little regulation of the Internet; (iii) anonymity; (iv) low costs; (v) low barriers to entry; (vi) multimedia capabilities; and (vii) the ability to widely reach potential audiences.

Terrorist organizations worldwide use the Internet to host websites in a number of countries and for a number of different purposes, all of which pose a challenge to law enforcement agencies. Some of these purposes are: (i) psychological warfare; (ii) publicity and propaganda; (iii) data-mining; (iv) fundraising; (v) recruitment and mobilization; (vi) radicalization; (vii) networking; (viii) information sharing; and (ix) planning and coordination. Lim then explained a number of possible ways to usefully monitor and collect actionable information on websites. These may include the use of link analysis and content analysis to gain a better picture on how certain websites, or groups of websites, are being utilized.

Lim then explored some of the emerging ways communication technologies — specifically mobile phones — are being used by terrorists. The most troublesome one for law enforcement agencies is the use of downloadable encryption programs for voice and data encryption and the use of Voice-over-Internet-Protocol (VOIP) services, which are difficult for law enforcement agencies to effectively monitor.

One of the most difficult issues arising out of the increased use of information and communication technologies, Lim noted, were problems in sharing telephone records between countries. As terrorists increasingly connect virtually across borders using the Internet or cheap mobile phones, the ability to match numbers to an international database becomes more important. Lim stated that solutions to

this and other investigative issues are legally complex, technologically problematic, and ethically ambiguous. There exists significant gaps in international cooperation and, because of the emerging issues surrounding the use of information and communication technologies in terrorism, there is an urgent need to create information and intelligence-sharing mechanisms among law enforcement and security agencies at the regional or international level.

Alexander Lim talking about the influence of information and communication technologies on terrorist activities.

RMA Redux: The Promise and Peril of Information and Communication Technologies

Paul Mitchell looked at the impact of information and communication technologies (ICT) on national security, examining it from a military perspective by using the theoretical lens of what is called the Revolution in Military Affairs (RMA). He opened his discussion by noting that it is a multidisciplinary problem that is often too narrowly examined by stove-piped disciplines. Examining the impact of ICT through previous work on RMA may illuminate some of the issues at work because much of early discussions about revolutions and the impact of technology on military affairs mirror current debates about the impact of ICT.

Contemporary interest in RMA dates back about 15 years, with the dramatic impact of the success and low loss of lives encountered in Desert Storm, which seemed to signal a shift in the efficacy of battle itself. Underlying the impact of Desert Storm and its influence on recent RMA literature is the German blitzkrieg operations in the invasion of France in 1940. There was a sense after Desert Storm that a similar military shift was taking place and nation states did not want to suffer the same fate as France.

During the 1950s, similar questions were being asked about the impact of nuclear weapons on the military. At that time, nuclear weapons were a novel technology. There was no history and no data points about what it would mean for the military, resulting in pure speculation about their impact. This resulted in the rise of, for example, the "Pentomic Division" in the United States — an ultimately unworkable and quickly discarded operational idea.

Mitchell questioned whether, in light of what we now know about nuclear weapons, an information-led modern RMA was as equally dubious in terms of its impact on tactics and strategy. However, he noted that the role of information in general and ICT in particular is much broader than nuclear weapons in that it is affecting both society and the military.

To help explain what kinds of shifts might be occurring in society, Mitchell discussed the work of the sociologist Manuel Castells and his study of the network society in which he developed the notion of "informationalism." This is simply the technological paradigm that underlies the emerging social change that is taking place. Informationalism is a combination of three features easily seen by even casual observers of ICT. Mitchell explained that these are: (i) the expanding processing power of information systems ("Moore's Law"), which lowers costs and enables more computing power to be put to use in everyday life; (ii) the mutability and recombinant nature of digital information

that allows for it to be repurposed and used in an ever-expanding variety of uses; and (iii) distributional flexibility in the growth and spread of networks distributing the information generated by the first two forces.

In such a way, informationalism generates the self-reflexive development of more information and thus builds upon itself in a continuous process. It engenders a creative and innovative process that promises a radical liberation of both human and institutional agency. Considering the major strategic issues confronting developed militaries around the globe, this would seem an ideal construct for things like the prosecution of the war on terror and other global military operations, as well as more specialized missions such as missile defense and homeland security. Such a capability, however, can just as easily generate centralized micro management as any mission-oriented decentralized decision-making for tactical units. Thus, there are significant barriers that may frustrate militaries in specific and governments in general in their ability to realize the benefits of digital technology.

Paul Mitchell presenting the impact of information and communication technologies on national security from an RMA perspective.

Discussion

A participant noted that technology is a pervasive part of the military, and the face of the modern RMA is technology, even if there are a number of other important forces at work. However, the participant questioned if technology had become so pervasive that technology had become a strategy in itself, rather than an aid to strategy. A speaker responded that because technology is fairly easy to understand and one could largely control and plan for its development, trying to deal with the social, political and economic problems that are the basis of warfare are much more difficult. It is easy, the speaker continued, to default to clean tactical solutions rather than deal with the messiness that many modern situations militaries are confronted with. Indeed, the speaker noted, the amount of money increasingly spent by modern military establishments on new technologies leads to the question of the strategy behind such purposes and whether there are non-technical solutions to solving some of the problems that militaries — and nations — are tasked with.

Another participant, noting the proliferation of government white papers on information sharing as well as recent cyber-security events in Estonia and elsewhere, asked whether such collaboration in the cyber-realm and information sharing is an increasing necessity. A speaker responded that he saw zero chance of any such real collaboration based on their research into previous attempts at military collaboration. Agreeing with the participant that a number of nations had been talking about the importance of information sharing and collaboration for a number of years, the speaker noted that these policy statements had not been operationalized in any meaningful way. One of the important, and misunderstood, problems in this area is that information sharing and collaboration is not a technical problem, but a human one. Connecting information together is not a problem, but social relationships are. Sharing national secrets is an issue of trust, and trust is not something nation-states do very well.

PANEL 4:

Other Technologies and Wild Cards

Use It or Loose It Or An Ideas Race

Kevin Dean started his presentation by stating that a situation of war has introduced a potential competitive process in the arms race with terrorists. Dean noted that present-day terrorists are willing to use any type of technology that works and authorities have been forced to continually react to such threats so far. He suggested that reaction is not necessarily the best way to deal with such situations and authorities should aim to reach the stage where they are able to pre-empt and infiltrate the terrorist system.

With regard to the threat of Improvised Explosive Devices (IED), Dean noted that several countries — including Australia and the United States — had already spent approximately USD 20 billion on ways to alleviate the problem with limited success. He proceeded to list readily available items that could potentially be used by terrorists to kill, including industrial by-products such as petroleum, rubber, plastics and metal, and industrial waste products such as carbon black, commonly used to make tires.

In detailing what he referred to as near-term threat technologies, Dean listed the presence of technologies such as fuel/air explosive enhancements capable of taking out the side of an aircraft. He revealed that authorities were aware of the fact that Al Qaeda and the Taliban had been recruiting biologists, signalling the possibility that they were becoming interested in biological processes. Dean illustrated that such technologies are within the reach of ordinary civilians, noting the proliferation of bio-clubs on the Internet that disseminate information on how to start a biological nurturing lab in a garage with readily available materials. Basically, the actual concept of splicing a carrier and an effective agent is becoming known, with people able to perform these experiments in their garage.

Dean proceeded to raise the possibility of creating disruptive functions at the quantum level. It appeared that the potential for change and disruption within the social structures of the world would be dependant on the quantum effects that scientists were beginning to look at, and this technology could probably surface within the next 15 years. According to Dean, another area of interest to consider is psychology, which is equally significant as technology is of no use without humans. Dean stated that while technology is the way of doing something, human inter-relationships are the context in which this would take place.

Dean concluded his presentation by stating that quantum technology would be responsible for significant changes in the future. In terms of biotechnology, advances in this area in the year 2030 and beyond would be able to provide human beings with the possibility of staying alive longer, basically allowing for a generational process beyond the normal human lifespan. In the area of developing technology, Dean highlighted the possible future use of nano-explosives, psychotropic substances, directed energy and cyber attacks.

Kevin Dean sharing his knowledge about various types of technologies which may pose a threat to the national security.

Current and Emerging Use of Dual-user Technologies

Rohan Gunaratna began his presentation by highlighting the fact that the threat of terrorism had grown significantly after the September 11 attacks. He stated that the single biggest change during that period was the fact that Al Qaeda had been spreading and sharing their knowledge and ideology with about 30 to 40 different groups in Asia, Africa and the Middle East. Touching on the capabilities of Al Qaeda, Gunaratna noted that one of the most important

committees within the organization is the military committee, with dedicated departments for technological acquisition and research. The organization has also formed a Weapons of Mass Destruction Committee led by the organization's expert on Improvised Explosives Devices (IEDs), who also designed the shaped charge that was used in the USS Cole attack.

To illustrate the types of technology used in terrorist attacks, Gunaratna referred to two types of explosives known to have been used by British terrorist cells, Hexamethylene Triperoxide Diamine (HMTD) and Triacetone Triperoxide (TATP). According to Gunaratna, HMTD, also referred to as the "Mother of Satan" due to its highly unstable devices, was used during the 7 July 2005 attacks in London while TATP was used in the failed 21 July 2005 attacks. Both HMTD and TATP were developed by Palestinian groups and were later adopted by Al Qaeda. Gunaratna pointed out that materials used for both these explosives were commercially available and, in fact, could be built in garages and kitchens due to the availability of the materials and the methods for building the devices on the Internet. The use of HMTD and TATP was detected in a case in Australia a few months after the U.K. attacks with remarkable similarities between both the U.K. and Australian cases.

Gunaratna then turned his attention to Southeast Asia, noting that while the terrorists here do not go down the route of using HMDT and TATP, they are known to use various types of technologies that have proven to be more sophisticated. To illustrate his point, Gunaratna referred to the example of Hambali, who planned an aviation attack after September 11. Hambali's plan involved the use of a shoe bomb that was designed to breach airplane cockpit doors, which had been strengthened after the September 11 attacks. The device was made in Thailand by an Al Qaeda cell. While Hambali's plan did not progress due to his arrest in a joint U.S.-Thai operation, the technology subsequently made its way to the United States.

Gunaratna stated that countries such as China, Singapore, Malaysia, Indonesia, Hong Kong and Taiwan are becoming increasingly important to terrorist groups in Asia in their quest to obtain technology. He further noted the significant movement of technology from North Korea and China to the Liberation Tigers of Tamil Ealam (LTTE) based in Sri Lanka. Accordingly, the LTTE had been able to obtain technology from many countries in Asia through purchasing ships from Japan, boat designs from Australia and equipment from Singapore. However, the primary source of technology for the LTTE came from North Korea and China.

In conclusion, Gunaratna foresaw that the terrorist threat would continue spreading in the future and advocated a greater sharing of intelligence and indicators between government and the private sectors in combating such threats.

Rohan Gunaratna sharing his findings on the ability of terrorists to use technology for malicious purposes.

Harnessing Science and Technology to Defeat Unconventional Threats

Lim Kian Boon began his presentation by emphasizing the importance of having technology-savvy officers who would be able to adopt and harness technology to the fullest. He pointed out, however, that technological advancement alone was not sufficient as it was imperative to integrate it with operational capabilities.

Lim noted that events in the last decade, such as the attacks on 11 September 2001, the Severe Acute Respiratory Syndrome (SARS) epidemic, incidents of letters mailed with anthrax spores, and home-made explosives had shaped the way authorities view future security threats. He stressed the challenges of assessing the likelihood of such threats in order to ensure readiness to deal with the eventualities and to be able to minimize the damage. For Lim, the use of science and technology provides a strong baseline in understanding the challenges faced and also assists in

the development of control measures used in minimizing the occurrences of threats. To elaborate on his point, Lim referred to the fact that, presently, terrorists no longer use conventional mechanical devices, but are instead looking towards energetic reactions for explosions due to the fact that mechanical devices are now easier to detect. To counter this, the identification of the list of possible materials and technologies used will allow government agencies to detect possible abuses through ensuring tighter control of inventories.

In dealing with unconventional threats, Lim noted that frontline officers would prefer to have devices with universal detection capabilities that are able to detect hazardous materials. However, this is not possible with today's technological advancements, but can be overcome with an appreciation of the strengths and limitations of current technology, which would allow for the intelligent and coordinated use of detection methods. To illustrate, Lim stated that it would be pointless to deploy walk-through metal detectors together with millimeter-wave detection systems because both are physical detectors. Rather, a combination of physical detectors with explosive trace detection systems should be used to broaden the scope of the detection capabilities. He also noted that it was better to invest in capabilities that provided continuous upgrading, which would maximize the operational life and potential of the technology.

Lim stressed that interception and mitigation capabilities should go hand in hand and that the greatest concern for frontline security personnel at present is to mitigate or contain possible explosive devices. Thus, frontline officers need to be equipped with mitigation measures that are easy to carry, such as compressible and easily compactable shock-absorbent materials that can be deployed quickly when a bomb threat is detected.

In sum, Lim concluded his presentation by emphasizing again the importance of harnessing the use of science and technology in enhancing operational capabilities, noting that it needed to be accomplished through long-term funding and research as well as development initiatives.

Lim Kian Boon suggesting how we can harness science and technology to prevent terrorist threat.

Discussion

A participant raised the question about Operation Crevice, which was a raid launched by the police force in England in 2004 in response to a report that there might be a Pakistani terrorist cell in England conspiring to launch a terrorist attack using an explosive. She asked a speaker what it revealed about the skill sets of the terrorists involved. A speaker answered that while the cell members investigated under Operation Crevice were not entirely competent, the knowledge of the Al Qaeda cell in the United Kingdom proved to be surprising. They were able to access individuals with specialist knowledge that gave them an advantage. A speaker was of the opinion that there is now a new generation of educated terrorists who are able to access information that is needed. Some of these terrorists may be scientists, working in facilities that are well controlled. Therefore, new layers of security features are necessary to prevent them from getting access to such specialist knowledge.

To the question of whether current trends reveal terrorists are mimickers or innovators, a speaker opined that most terrorists are imitators and not innovators. However, he also pointed out that they are creatures of necessity and are driven by the surrounding environment.

ROUNDTABLE DISCUSSION:

Lessons Identified and the Way Forward

The first issue addressed during the roundtable discussion highlighted the technological trends and developments for national security practitioners' attention. A key challenge currently facing governments is the difficulty in monitoring the abuse of sophisticated commercial-off-the-shelf (COTS) technology by enemies of the state as it becomes increasingly accessible to non-state actors. Technological advances harnessed for worthy causes may also have unintended national security consequences. For example, health technology that enhances longevity may result in demographic challenges such as youth bulges in developing countries and aging populations in developed countries. To better ride the technological wave, it was recommended that governments complement their investment in the development and tracking of new technology with social scientists to assess its utility and potential threats to the state.

The second issue pertained to forging effective working relationships between scientists and technologists on the one hand and governments on the other. This involved the production of policy-relevant advice from technologists and scientists, and for policymakers to formulate good policies from it. Some of the challenges to generating actionable policy briefs include: (i) the difficulty for policymakers to make sense of scientific and technical jargon in reports by scientists; (ii) the lack of awareness of the needs of, and contexts faced by, policymakers; and (iii) the problem of timing as policymakers require quick solutions to address current problems while scientists often need a lot more time to develop their work. To alleviate some of these barriers, it was suggested that analysts who are able to facilitate communication between the two camps be recruited. Alternatively, scientists and engineers can be given opportunities to move in policy circles to better grasp the needs of policymakers.

The third issue related to harnessing science and technology to defeat terrorist networks and transnational organized crime groups. It was noted that more attention needed to be paid to the human factor, namely fostering mechanisms for better cooperation and including technologically competent individuals in the policy-making process. To achieve these objectives, it was suggested that opportunities be created for developing bilateral and regional partnerships to share ideas through processes such as Track II science diplomacy and for governments to focus more on seizing the initiative to effect positive changes than on fighting its potential negative impacts.

Participants actively engaged in syndicate group discussion.

Workshop Program

Sunday, 13 September 2009

1700 – 1900 hrs **Arrival of Invited Foreign Participants and Speakers**

Venue: Marina Mandarin Hotel

1900 – 2100 hrs **Welcome Reception**
Hosted by:
Lee Ark Boon, Director,
National Security Coordination Centre
National Security Coordination Secretariat
and
Warren Fishbein, US Coordinator
Global Futures Forum
US Department of State

Monday, 14 September 2009

0800 – 0900 hrs **Registration**

0900 – 0910 hrs **Welcome Remarks by Ambassador Barry Desker**
Dean
S. Rajaratnam School of International Studies (RSIS), NTU
Venue: Vanda Ballroom (Level 5)
Attire: Lounge Suit (Jacket and Tie)

0910 – 0920 hrs **Welcome Remarks by Susan H. Nelson**
Director
Office of Outreach in the Bureau of Intelligence, and Research (INR/OTR)
U.S. Department of State

0920 – 0930 hrs **Opening Address by Lui Pao Chuen**
Chief Scientific Advisor
Ministry of Foreign Affairs
Advisor
National Research Foundation and
Consultant to Ministry of Defence, Singapore

0930 – 1015 hrs **Keynote Speaker**
"Avoiding Technology Surprise: Measures and Countermeasures"
Ruth David, President and CEO, ANSER

1015 – 1045 hrs Tea Break

1045 – 1230 hrs **Panel One — Innovation and Globalization**

Venue: Vanda Ballroom (Level 5)
Attire: Smart Casual (Long-sleeve shirt without tie)

Chairperson:
Kumar Ramakrishna
Head
Centre of Excellence for National Security (CENS), RSIS, NTU

Speaker:
"***Disruptive Technologies: Redefined"***
George Atkinson
Director
Institute for Science and Global Policy, &
Professor of Chemistry and Optical Sciences, University of Arizona, USA

"Emerging Technologies, Sustainable Development, and Stability"
Richard Silberglitt
Senior Physical Scientist, RAND Corporation & Chair, International Advisory Board, APEC Center for Technology Foresight

Question & Answer

1230 – 1330 hrs Lunch

Venue: Pisces & Aquarius Ballroom (Level 1)

1330 – 1530 hrs **Panel Two — Dual Technologies and ICT (I)**

Venue: Vanda Ballroom (Level 5)
Attire: Smart Casual (Long-sleeve shirt without tie)

Chairperson:
Susan H. Nelson
Director
Office of Outreach in the Bureau of Intelligence, and Research (INR/OTR), U.S. Department of State

Speaker:
"Nanotechnology, Ecosystems and Urban Infrastructure"
Terry Turney
Professorial Fellow
Centre for Green Chemistry
Monash University, Australia

"Bionanotechnology and Security: Is Small Scary?"
Margaret Kosal
Assistant Professor
Sam Nunn School of International Affairs
Georgia Institute of Technology

"Dual Use Issues and Education for Life Scientists"
Nariyoshi Shinomiya
Professor
Department of Integrative Physiology and Bio-Nano Medicine
National Defense Medical College, Japan

"Evolving Tactics — Exploiting Advances in Simulation and Machine Learning Technologies"
How Khee Yin
Director
Information Division, DSO, Singapore

Question & Answer

1530 – 1545 hrs Tea Break

1545 – 1700 hrs Panel Three — Dual Technologies and ICT (II)

Venue: Vanda Ballroom (Level 5)
Attire: Smart Casual (Long-sleeve shirt without tie)

Chairperson:
Cung Vu
Defense Warning Office
Global Futures Forum
U.S. Department of State

Speaker:
"Terrorist Use of Information Technology and Implications for Counter-Terrorism Policies"
Alexander Lim
Criminal Intelligence Analysis, INTERPOL Liaison Office, Bangkok

"RMA Redux: The Promise and Peril of Information and Communication Technologies"
Paul Mitchell
Department of Defence Studies
Canadian Forces College

1700 – 1715 hrs Wrap Up

1715 hrs End of Day Two

1830 – 2100 hrs Welcome Dinner

Venue: Pool Garden (Level 5, Pool side)
Attire: Smart Casual (Long-sleeve shirt without tie)

Tuesday 15 September 2009

0815 – 0845 hrs Registration

0845 – 0900 hrs Review of Day Two
Cung Vu
Defense Warning Office
Global Futures Forum
U.S. Department of State

Venue: Vanda Ballroom (Level 5)
Attire: Smart Casual (Long-sleeve shirt without tie)

0900 – 1030 hrs **Panel Four — Other Technologies and Wild Cards**

Venue: Vanda Ballroom (Level 5)
Attire: Smart Casual (Long-sleeve shirt without tie)

Chairperson:
Jerry Everard
Director
Emerging Technologies
Department of Defence
Canberra, Australia

Speaker:
"USE IT or LOOSE IT (or an Ideas Race)"
Kevin Dean
Senior Scientist
Defence Science and Technology Organisation
Australia

"Current and Emerging Terrorist Use of Dual User Technologies"
Rohan Gunaratna
Head
International Centre for Political Violence and Terrorism Research, RSIS, NTU

"Harnessing Science and Technology to Defeat Unconventional Threats"
Lim Kian Boon
Senior Assistant Director (Partnerships),
Office of the Chief Science and Technology Officer (OCSTO)
Ministry of Home Affairs

Question & Answer

1030 – 1100 hrs Tea Break — Network Time

1100 – 1230 hrs Syndicate Group Discussion

Venue: Vanda Ballroom (Level 5),
Vanda 3, 4 & 5 Meeting Rooms (Level 6)

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

1230 – 1330 hrs Lunch — Network Time

Venue: Pisces & Aquarius Ballroom (Level 1)

1330 – 1415 hrs Syndicate Group Discussion

Venue: Vanda Ballroom (Level 5), Vanda 3, 4 & 5 Meeting Rooms (Level 6)

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

1415 – 1615 hrs **Putting It All Together: Lessons Identified and the Way Forward (Roundtable Discussion / Closing Panel)**

Chairperson:
Andrew W. Reynolds
Deputy S&T Adviser to the Secretary of State
U.S. Department of State

Venue: Vanda Ballroom (Level 5)
Attire: Smart Casual (Long-sleeve shirt without tie)

Question and Answer

1615 hrs Closing Remarks by **Warren Fishbein**

1630 hrs Tea Reception

1800 hrs Network and Family Outing (Optional – Family and Guests) Night Safari

Venue: Singapore Zoological Gardens

Participants

List of Presenters and Chairpersons

Presenters

1. **George Atkinson**
   University of Arizona
   Professor of Chemistry and Optical Sciences
   Director, Institute on Science for Global Policy
   College of Science, Gould Simpson Building,
   Room 1025, PO Box 210077,
   1040 E. 4th Street, University of Arizona,
   Tucson, Arizona 85721-0077
   Email atkinsonga@mindspring.com

2. **Ruth David**
   President and Chief Executive Officer
   Analytic Services Inc.
   2900 South Quincy Street,
   Suite 800, Arlington,
   VA 22206
   Email ruth.david@anser.org

3. **Kevin Dean**
   Senior Scientist
   Defence Science and Technology Organisation
   Australia
   Email Kevin.Dean@dsto.defence.gov.au

4. **Rohan Gunaratna**
   Head
   International Centre for Political Violence and
   Terrorism Research (ICPVTR)
   S. Rajaratnam School Of International Studies
   Nanyang Technological University
   Block S4, Level B4, Nanyang Avenue
   Singapore 639798
   Email isrkgunaratna@ntu.edu.sg

5. **How Khee Yin**
   Director of Information Division
   DSO
   20, Science Park Drive
   Singapore 118230
   Email hkheeyin@dso.org.sg

6. **Margaret Kosal**
   Professor
   Georgia Institute of Technology
   781 Marietta Ave NW
   Atlanta GA 30332-0610 USA
   Email margaret.kosal@inta.gatech.edu

7. **Alexander Lim**
   Criminal Intelligence Analyst
   I.C.P.O INTERPOL General Secretariat
   Bangkok
   12 Floor, Building 19
   Rama 1 Road, Patumwan
   Bangkok 10330, Thailand
   Email a.lim@interpol.int

8. **Lim Kian Boon**
   Senior Assistant Director (Partnerships)
   Office of the Chief Science &
   Technology Officer (OCSTO)
   Ministry of Home Affairs
   Republic of Singapore
   Email Lim_Kian_Boon@mha.gov.sg

9. **Paul Mitchell**
   Department of Defence Studie
   Canadian Forces College
   Email mitchell@cfc.dnd.ca

10. **Nariyoshi Shinomiya**
    Professor
    National Defense Medical College
    Department of Integrative Physiology and
    Bio-Nano Medicine
    National Defense Medical College
    3-2 Namiki, Tokorozawa,
    Saitama 359-8513, Japan
    Email shinomi@ndmc.ac.jp

11. **Richard Silberglitt**
    Senior Physical Scientist
    Rand Corporation
    1200 South Hayes Street
    Arlington, VA 22202-5050 USA
    Email Richard@rand.org

12. Terry Turney
Professorial Fellow
Centre for Green Chemistry
Monash University
Clayton, Victoria
Australia 3800
Email terry.turney@sci.monash.edu.au

Chairpersons & Key Participants

13. Barry Desker
Dean
S. Rajaratnam School Of International Studies
Nanyang Technological University
Block S4, Level B4, Nanyang Avenue
Singapore 639798
Email isbdesker@ntu.edu.sg

14. Jerry Everard
Director, Emerging Technology
Department of Defence,
Canberra Australia
Email jerry.everard@defence.gov.au

15. Warren H. Fishbein
US Coordinator
Global Futures Forum
US Department of State
Email FishbeinWH@state.gov

16. Lee Ark Boon
Director
National Security Co-ordination Centre
National Security Co-ordination Secretariat
5 Maxwell Road
#15-00 Tower Block
MND Complex
Singapore 069110
Email Lee_Ark_Boon@nscs.gov.sg

17. Lui Pao Chuen
Chief Scientific Advisor
Ministry of Foreign Affairs
Advisor
National Research Foundation
Consultant to Ministry of Defence
Singapore
Email Lui_pao_chuen@starnet.gov.sg

18. Susan H. Nelson
Director
Office of Outreach in the Bureau of Intelligence and Research (INR/OTR)
U.S. Department of State
Email NelsonSH@state.gov

19. Kumar Ramakrishna
Head
Centre of Excellence for National Security
S. Rajaratnam School Of International Studies
Nanyang Technological University
Block S4, Level B4, Nanyang Avenue
Singapore 639798
Email iskumar@ntu.edu.sg

20. Andrew W. Reynolds
Deputy S&T Adviser to the Secretary of State
U.S. Department of State
Email ReynoldsAW@state.gov

21. Cung Vu
Defense Warning Office
Global Futures Forum
U.S. Department of State
Email Cung.Vu@dia.mil

List of Participants

A* Star Institute of Infocomm Research
1 Fusionopolis Way, #21-01 Connexis (South Tower)
Singapore 138632

22. Gerard Ang
Senior Manager (Industry Development
Email Gerard@i2r.a-star.edu.sg

Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS)
Blk S4, Level B4, Nanyang Avenue
Singapore 639798

23. Yolanda Chin
Associate Research Fellow
Email istlchin@ntu.edu.sg

24. Gregory Dalziel
Associate Research Fellow
Email isgdalziel@ntu.edu.sg

25. Bill Durodie
Senior Fellow
Email iswdurodie@ntu.edu.sg

26. Clint R. Lorimore
Associate Research Fellow
Email iscrlorimore@ntu.edu.sg

27. Ng Sue Chia
Associate Research Fellow
Email issuechia@ntu.edu.sg

28. Jenna Park
Associate Research Fellow
Email isjhpark@ntu.edu.sg

29. Norman Vasu
Deputy Head, CENS
Email isnvasu@ntu.edu.sg

30. Yeap Su Yin
Associate Research Fellow
Email issyyeap@ntu.edu.sg

Defence Science & Technology Agency (DSTA)
71 Science Park Drive #02-05
Singapore 118253

31. Sin Bon Wah
Deputy Chief Executive (Special Duties)
Assistant Director (Defence Policy Office)
Email sboonwah@dsta.gov.sg

32. Tan Peng Yam
Deputy Chief Executive (Operations)
Email tpenyam@dsta.gov.sg

Defence Science & Technology Agency (DSTA)
RAHS Experimentation Centre
5 Maxwell Road, #12-00 Tower Block
MND Complex, Singapore 069110

33. Tan Kwan Chong
Engineer (National Security Solutions)
Networked System
Email tkwancho@dsta.gov.sg

CLAR, Defense Warning Office
DWO, Bldg 6000
Washington DC 20340, USA

34. Courtney Cho
Email unyoung.cho@dia.mil

Department of Homeland Security
USA

35. Joel D. Wall
Email joel.wall@dhs.gov

Department Defence
Australia

36. Jerry Everard
Director, Emerging Technology
Email jerry.everard@defence.gov.au

Embassy of the United States of America
27 Napier Road
Singapore 258508

37. Jeemes L. Akers
First Secretary
Email akersjl@state.gov

38. Joe Johnson
Associate Director, Ocean, Atmosphere and Space
Office of Naval Research Global
Email joseph.johnson@onrasia.navy.mil

39. Sandra F. Maynard
Political/Military Officer
Email MaynardSF@state.gov

Jane's Information Group
78 Shenton Way #12-01
Singapore 079120

40. Jim Head
Regional Channel Consultant
Asia Pacific
Email jim.head@janes.com

Joint Counter-Terrorism Centre (JCTC)
5 Maxwell Road
#15-00 Tower Block
MND Complex
Singapore 069110

41. Luke Ho
Research Analyst
Email Luke_Ho@nscs.gov.sg

42. Lim Cheng Yong
Assistant Director (Research)
Email Lim_Cheng_Yong@nscs.gov.sg

43. Sunit Singh
Research Analyst
Email Sunit_Singh@nscs.gov.sg

Ministry of Defence
303 Gombak Drive #05-05
Singapore 669645

44. Chris Leck
Assistant Director (Defence Policy Office)
Email chris_leck@mindef.gov.sg

45. Lim Soon Chia
Deputy CRTo (O)/C4 & Deputy HJPT (T)
Defence Research Techonology Office
Email soonchia@starnet.gov.sg

Ministry of Home Affairs
28 Irrawaddy Road
Singapore 329560

46. Chee Kwok Min
Assistant Director (Partnerships)
Office of the Chief Science & Technology Officer
Email chee_kwok_min@mha.gov.sg

47. Kee Shwu Yee Krystin
Deputy Director
Email kee_shwu_yee@mha.gov.sg

48. Kenneth Lau Yip Choy
1 Manager (Techonlogy Development)
Technology & Infrastructure Division
Email Kenneth_lau@mha.gov.sg

49. Leow Shee Yin
Assistant Director (Partnerships)
Office of the Chief Science & Technology Officer
Email leow_shee_yin@mha.gov.sg

50. Teo Ban Sim
Senior Consultant
Infocomm Development Authority of Singapore
Email bansim.teo@gmail.com

National Security Coordination Centre (NSCC)
5 Maxwell Road
#15-00 Tower Block
MND Complex
Singapore 069110

51. Bobby Fay
Deputy Director (Strategic Plans & Resource)
Email Bobby_Fay@nscs.gov.sg

52. Sean Lee
Deputy Director (Policy And International Relations)
Email Sean_lee@nscs.gov.sg

53. Wesley Lim
Executive (RAHS)
Email Wesley_Lim@nscs.gov.sg

54. Patrick Nathan
Deputy Director (Policy And International Relations)
Email Patrick_Nathan@nscs.gov.sg

55. Kim Ong-Giger
SAD (HSC)
Emai Ong-Giger_Kim@nscs.gov.sg

56. Edna Tan
Assistant Director (RAHS)
Email Edna_Tan@nscs.gov.sg

57. Tan Soon Kuan
Assistant Director (RAHS)
Email Toh_Soon_Kuan@nscs.gov.sg

Public Service Division
Prime Minister's Office
100 High Street #07-00
The Treasury
Singapore 179434

58. Aaron Maniam
Deputy Director, Strategic Policy
Public Service Division, Prime Minister's Office
Email Aaron_Maniam@psd.gov.sg

Nexus, Ministry of Defence (MINDEF)
5 Depot Road #10-01
Defence Technology Tower B Singapore 109681

59. Chua Kun Jie
Staff Writer
Email kjchua@gmail.com

60. Lim Kok Siong
Director Nexus
Email lim_kok_siong@mindef.gov.sg

61. Loo Xue Mei
Research Officer (Current Issues)
Email Loo_Xue_Mei@starnet.gov.sg

62. Ong Kheng Hoe
Deputy Director (Programme @ Development)
Email ong_kheng_hoe@starnet.gov.sg

S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University
Block S4, Level B4, Nanyang Avenue
Singapore 639798

63. Raman Venkateshwaran Anand
MSc Student
Email R090005@ntu.edu.sg

64. Jan Eichstedt
MSc Student
Email JANE0008@ntu.edu.sg

65. Keith Eric Flick
PhD Student
Email KEIT0004@ntu.edu.sg

66. Karunya Jayasena
Research Analyst, ICPVTR
Email karunya.jayasena.674@csun.edu

67. Amos Khan
Research Analyst
Email isamoskhan@ntu.edu.sg

68. Adrian Kuah
Associate Research Fellow, IDSS
Email iswjkuah@ntu.edu.sg

69. Le Wenjing
MSc Student
Email R090024@ntu.edu.sg

70. Chen Lei
MSc Student
Email CHEN0705@ntu.edu.sg

71. Long Xuan
MSc Student
Email LONG0027@ntu.edu.sg

72. Marc Gilbert Villot
MSc Student
Email VILL0001@ntu.edu.sg

73. Muhammad Shafqat Munir
Research Analyst, ICPVTR
Email issmunir@ntu.edu.sg

74. Ong Wei Chong
Associate Research Fellow, IDSS
Email iswcong@ntu.edu.sg

75. Phua Pei Pei
MSc Student
Email R090018@ntu.edu.sg

76. Thamapon Rajchawang
MSc Student
Email THAN0046@ntu.edu.sg

77. Sim Lee Koon Susan
Adjunct Senior Fellow
Email issusansim@ntu.edu.sg

78. Muthusaravanan s/o Sivasubramaniam
MSc Student
Email MU0003AM@ntu.edu.sg

79. Yadgarov Sherali
Research Analyst, ICPVTR
Email isysheralil@ntu.edu.sg

80. Annabella Belanie Gloria Spittel
Research Analyst, ICPVTR
Email isgspittel@ntu.edu.sg

81. Tian Hengyan
MSc Student
Email TI0001AN@ntu.edu.sg

82. Tor Erik Tjonneland
MSc Student
Email TORE0001@ntu.edu.sg

83. Wang Di
Research Analyst, IDSS
Email isdwang@ntu.edu.sg

84. Xiao Xialian
MSc Student
Email XIAO0041@ntu.edu.sg

85. Xun Bin
MSc Student
Email XUNB0001@ntu.edu.sg

86. Yoon Seung Pyo
MSc Student
Email YOON0006@ntu.edu.sg

87. Zhang Ting
MSc Student
Email R090017@ntu.edu.sg

About GFF

What Is GFF?

The Global Futures Forum (GFF) is a multinational community initiated in 2005 that works at the open source level to identify and make sense of transnational threats. Its primary goal is to foster the development of enhanced insight and foresight among its membership through the exchange of different perspectives and through the utilization of collaborative research tools.

Who Is GFF?

GFF seeks to involve a diverse population of officials and subject-matter experts to stimulate cross-cultural and interdisciplinary thinking, and to challenge prevailing assumptions. GFF participants include government security officials, along with security-related experts from the academia, non-government organizations, and industry. More than 1,000 officials and experts from over 40 countries have taken part in GFF activities.

How Does GFF Work?

Face-to-Face Meetings

General Meetings: Washington in 11/2005, Prague in 12/2006, Vancouver in 4/2008, and Singapore in mid-2010.

Community of Interest Workshops: Small, topic-based meetings held regularly in various member countries.

GFF operates a password-protected website that is the repository of GFF production, including hundreds of readings and resources on relevant topics, member blogs, discussion forums, and wikis.

What are GFF Areas of Interest?

Current GFF communities of interest include Radicalization, Practice and Organization of Intelligence, Illicit Trafficking, Strategic Foresight and Warning, Terrorism and Counter-terrorism Studies, Proliferation, and Emerging and Disruptive Technologies.

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

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, strategizing 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 strategizing 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 four main domains:

Radicalization Studies

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

Social Resilience

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

Homeland Defence

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

Futures Studies

- The study of various theoretical and conceptual approaches to the systematic and rigorous study of emerging threats, as well as global trends and opportunities — on the assumption that Resilience also encompasses robust visions of the future.

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 organizes courses, seminars and workshops for local and foreign national security officials to facilitate networking and exposure to leading-edge thinking on the prevention of, and response to, national and homeland security threats.

How Does CENS Help Raise Public Awareness of National Security Issues?

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

How Does CENS Keep Abreast of Cutting Edge National Security Research?

The lean organizational 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 links to "Centre of Excellence for National Security"

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 the Deputy Prime Minister Professor S. Jayakumar, who is also Minister for Law.

NSCS is headed by Permanent Secretary (National Security and Intelligence Coordination). The current PS (NSIC) is Mr. Peter Ho, who is concurrently Head of Civil Service and Permanent Secretary for Foreign Affairs.

NSCS provides support to the ministerial-level Security Policy Review Committee (SPRC) and Senior official-level National Security Coordination Committee (NSCCom) and Intelligence Coordinating Committee (ICC). It organizes and manages national security programmes, one example being the Asia-Pacific Programme for National Security Officers. NSCS also funds experimental, research or start-up projects that contribute to our national security.

NSCS is made up of two components: the National Security Coordination Centre (NSCC) and the Joint Counter-Terrorism Centre (JCTC). Each center is headed by a director.

NSCC performs three vital roles in Singapore's national security: national security planning, policy coordination, and anticipating strategic threats. As a coordinating body, NSCC ensures that government agencies complement each other, and do not duplicate or perform competing tasks.

JCTC is a strategic analysis unit that compiles a holistic picture of terrorist threat. It studies the levels of preparedness in areas such as maritime terrorism and chemical, biological and radiological terrorist threats. It also maps out the consequences should an attack in that domain take place.

More information on NSCS can be found at **www.nscs.gov.sg**

About the S. Rajaratnam School of International Studies (RSIS)

The S. Rajaratnam School of International Studies (RSIS) was established in January 2007 as an autonomous School within the Nanyang Technological University (NTU). RSIS' mission is to be a leading research and graduate teaching institution in strategic and international affairs in the Asia-Pacific. To accomplish this mission, RSIS will:

- Provide a rigorous professional graduate education in international affairs with a strong practical and area emphasis
- Conduct policy-relevant research in national security, defence and strategic studies, diplomacy and international relations
- Collaborate with like-minded schools of international affairs to form a global network of excellence

Graduate Training in International Affairs

RSIS offers an exacting graduate education in international affairs, taught by an international faculty of leading thinkers and practitioners. The teaching programme consists of the Master of Science (MSc) degrees in Strategic Studies, International Relations, International Political Economy and Asian Studies. Through partnerships with the University of Warwick and NTU's Nanyang Business School, RSIS also offers the NTU-Warwick Double Masters Programme as well as The Nanyang MBA (International Studies). The graduate teaching is distinguished by their focus on the Asia-Pacific region, the professional practice of international affairs and the cultivation of academic depth. Over 200 students, the majority from abroad, are enrolled with the School. A small and select Ph.D. programme caters to students whose interests match those of specific faculty members.

Research

Research at RSIS is conducted by five constituent Institutes and Centres: the Institute of Defence and Strategic Studies (IDSS), the International Centre for Political Violence and Terrorism Research (ICPVTR), the Centre of Excellence for National Security (CENS), the Centre for Non-Traditional Security (NTS) Studies, and the Temasek Foundation Centre for Trade & Negotiations (TFCTN). The focus of research is on issues relating to the security and stability of the Asia-Pacific region and their implications for Singapore and other countries in the region. The School has three professorships that bring distinguished scholars and practitioners to teach and do research at the School. They are the S. Rajaratnam Professorship in Strategic Studies, the Ngee Ann Kongsi Professorship in International Relations, and the NTUC Professorship in International Economic Relations.

International Collaboration

Collaboration with other Professional Schools of international affairs to form a global network of excellence is a RSIS priority. RSIS will initiate links with other like-minded schools so as to enrich its research and teaching activities as well as adopt the best practices of successful schools.

For more information on the School, visit
www.rsis.edu.sg

S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

A Graduate School of Nanyang Technological University

Design by Oxygen Studio Designs

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