Global Futures Forum
General Meeting 2010

12-15 SEPTEMBER 2010
SINGAPORE

Global Futures Forum General Meeting 2010

Contents Page

BACKGROUND AND AIMS OF THE CONFERENCE

The Global Futures Forum General Meeting 2010, on the theme "Building Resilience in the Face of Future Shocks", featured various expert presentations and discussions primarily focused on improving understanding of the concept of national and societal "resilience", and especially on how intelligence analysis and strategic foresight can help to strengthen this vital capability. Resilience embraces such attributes as robustness (the ability of a nation or a community to withstand major shocks with as minimal disruption as possible), resourcefulness (real-time adaptiveness of governmental officials and citizens in responding to crises), and rapid recovery (the ability to bounce back quickly from major disruptions. The conference examined how various analytic techniques and processes, such as risk assessment and communication, and early warning of shocks-in-the-making could help governments and civil societies to develop better resilience in the face of increasingly complex transnational security challenges, including violent extremism and terrorism, pandemics, WMD proliferation and financial shocks.

In addition to the activities related to the General Meeting's central theme, there were also sessions exploring the GFF's recent and forthcoming projects in several substantive areas. These include radicalization and counterterrorism, analytic methods and training, illicit trafficking and cyber security.

Meeting participants also had an opportunity to provide input to the development of the GFF's future programs and were given generous opportunities for networking and face-to-face discussions.

WELCOME REMARKS BY DAVID ADELMAN

David Adelman, the **U.S. Ambassador to Singapore**, observed in his welcome remarks that new security challenges were different from previous ones. In the past, security threats were predominantly posed by identifiable state actors. Such traditional security threats still exist but new threats have emerged as a result of globalization and the information revolution with the advent of technological advances and the Internet. As a result, many threats that nations face today are posed by non-state actors, namely, terrorists, illicit traffickers and proliferation rings, who are difficult to pin down. While the "who", "what", "why" and "how" but not the "when" and "where" were known to past governments, the inverse is true today, as governments grapple more with the "who", "what", "why" and "how" more than the "when" and "where". Following from this, governments have been caught off-guard by "bolt out of the blue" security challenges over the recent past and this trend is likely to continue for the foreseeable future. Hence the onus is on governments to change the way they think to address these new challenges.

Commenting on the theme of the Global Futures Forum General Meeting, "Building Resilience in the Face of Future Shocks", Ambassador Adelman noted that the concept of resilience is an important element of the current U.S. national security strategy of the Obama administration. Recognizing the futility of deterring or preventing every single threat, the strategy called for the enhancement of resilience, defined as "the ability to adapt to changing conditions and prepare for, withstand and rapidly recover from the disruption".

Ambassador Adelman concluded with the observation that while the many different countries and institutions represented at the GFF had come to where they were from many different ways, everyone was "in the same boat" when it comes to new threats posed over the next century. One way to get ahead of the curve is to collaborate to share insights on how to tackle these new threats. In this respect, the GFF has the potential to be one of the leading platforms for this purpose as it brings together substantive experts from both government and non-government sectors from different countries to deliberate strategies to address the new threats facing nations this century.

WELCOME REMARKS BY MR. EDDIE TEO

In his welcome remarks, Mr. Eddie Teo, Chairman, Public Service Commission, highlighted the salience of the GFF theme, "Building Resilience in the Face of Future Shocks", in enhancing understanding of the multifaceted concept of national and societal resilience and the contributions of intelligence analysts to developing organic resilience.

Mr. Teo argued that resilience was important to national security professionals because they had a stake in understanding and helping to ensure that the society they lived in bounced back quickly from a crisis. How quickly a country recovers during the aftermath of a crisis indicates how resilient it is. Government policies must not only include the prevention of a terrorist attack or a pandemic outbreak but also address the issue of how quickly and completely societies recover from any national security crisis. Given this imperative, national security professionals need to reflect on how they define, understand, interpret, explain and put into practice the idea of "resilience" by critically examining the assumptions underpinning the concept.

In his conclusion, Mr. Teo noted that a major aim of the GFF was to bring together practitioners and academic specialists from across different domains to jointly address a range of transnational security issues. He hoped that these deliberations would lead to ongoing research projects and concrete follow-ups addressing the wide array of threats that nations face today and how the adoption of the strategic concept of resilience would strengthen nations' ability to overcome future shocks.

OPENING ADDRESS

In his opening address, Professor S. Jayakumar underscored the importance of deliberating the theme of the Global Futures Forum General Meeting, "Building Resilience in the Face of Future Shocks", given the current complex and unpredictable milieu facing governments today.

Four significant trends were identified. First, a new multi-polar compact will emerge due to the gradual shifting of power from the Atlantic to the Pacific, which will shape the future geopolitical landscape. Second, the continued threat of violent, extremist religious fundamentalism requires traditional security agencies to constantly adapt to new trends and for states to win the hearts and minds of people. Third, climate change will have grave economic, political and security repercussions such as the disruption of food and water supplies owing to volatile weather patterns and the destabilization of weak regimes due to ineffectual responses to catastrophic natural disasters. Fourth, as the world's population increases, competition for resources such as oil, food and water will intensify, resulting in increased tensions. Professor Jayakumar stressed that in dealing with these threats, traditional security frameworks and the efforts of individual nation states were inadequate and that collaboration among governments was essential.

Professor Jayakumar went on to outline three approaches adopted by Singapore to deal with these challenges. The first is to inculcate strategic foresight in government. In this complex and ever-changing global landscape, a linear, analytical approach to policy making alone is not sufficient. Governments need to go beyond mere efficiency in regulation to develop strategic foresight so that they can anticipate and proactively respond to such changes. Singapore has tried to achieve this over the years through programs such as Scenario Planning, and Risk Assessment and Horizon Scanning. Two lessons learnt from these efforts were the importance of experimentation and discovery, given that there is no single formula for developing a foresight capability, and the need for a collaborative and networked approach, namely, for the various ministries to discuss emerging issues and risks and share experiences on foresight projects and programs.

Second, Singapore has advocated a networked, whole-of-government approach, as its resources are limited and capabilities distributed. For example, with regard to Singapore's counter-terrorism strategy, the National Security Coordination Secretariat in the Prime Minister's Office was created in 2004 to coordinate national security policy and intelligence across various government agencies, while leaving the operational responses to the respective security agencies With regular exercises conducted to test security plans and strengthen inter-agency collaboration.

Third, a whole-of-society approach that engages academia, business, NGOs, the media and community groups is needed to fortify Singapore's social resilience. For example, in the area of critical infrastructure protection, the government has worked with private sector owners to jointly identify and analyze critical nodes, and assist them in making the necessary investment to enhance their resilience. Regular dialogues between ministers and the business community are held to get the latter to view security as an integral part of the business process and not a peripheral concern. At the

community level, the Community Engagement Program has been rolled out where five community clusters—religious groups, educational institutions, the media, grassroots organizations, businesses and unions—work together in a bottom-up effort. Emergency preparedness exercises are also organized regularly to test the readiness of our operational and community responses to terrorist attacks and other catastrophic events.

Nevertheless, Professor Jayakumar stressed that being in this for the long haul, Singapore needed to learn from the experiences and best practices of others to avoid fatigue and complacency setting in. In the area of building resilience, one can never do enough. Although no one would wish for their nation's resilience to be tested, in the face of an uncertain future and strategic challenges, one has to stand prepared for the worst.

LOOKING OUT FOR FUTURE SHOCKS

The panel examined best practices in strategic foresight. The presentations covered government projects in detecting emerging risks, analyses of energy foresight and lessons learnt from economic crises. In sum, effective foresight entailed a constant systematic effort for warning and risk identification that involves stakeholders well beyond the intelligence community and policymakers; the identification of anomalies or changes within the environment, rather than known events; and continued analyst development to identify and anticipate, evaluate, communicate, monitor and mitigate threats. Some of the challenges faced by governments to this end include cognitive bias, the failure of organizations to network and share, deep-seated mistrust of open-source intelligence, and analysts' inherent mistrust and fear of technology.

WARNING IN AN ERA OF EXTREME GLOBAL DYNAMISM

The speaker began with a reference to Hurricane Katrina, which struck New Orleans in 2005, to illustrate the importance of warning and risk management. He said that given the location, existing infrastructure and resources available to address catastrophic issues in New Orleans, the impact of Hurricane Katrina itself was not very surprising. What was surprising was how ill-prepared the U.S. community was in addressing this shock. Organizations in charge of monitoring the weather detected and flagged the impending disaster but what was lacking was the effort to take necessary and solid actions in response to the warning. This highlights the fact that merely providing warnings is not adequate in today's turbulent environment.

He argued that the fluctuation and turbulence in politics, the economy and technology contributed to the failure of warning systems as was seen in the case of Hurricane Katrina. Although there were experts who were engaged in their own field of expertise exclusively, experts capable of overseeing different areas in a holistic manner were lacking. He said that this expertise was crucial as these "different" areas were no longer disparate but interconnected in the present environment. The world is getting more and more difficult to understand, and intelligence has to deal with a host of real-world challenges that may sometimes be evident but often vague.

He opined that, compared to the past, the current global security was vaguely familiar, yet extremely different. In today's dynamic environment, merely providing warning was not enough and policymakers should be engaged at an early stage of the risk management process so as not to miss out on any available options. However, he said that before getting into serious discussions on risk management, there were several things that should be established at the fundamental level. First, there must be a constant systematic effort for warning and risk identification that involves stakeholders well beyond the intelligence community and policymakers. Second, it is important to always "walk the beat and stakeouts" to watch out for any anomalies or changes within the environment, rather than known events. Third, partnership should be valued over working in a subordinate relationship with a senior policymaker. Fourth, analysts must continuously improve their analytical skills and produce timely, relevant and actionable information through the following factors: identify and anticipate, evaluate, communicate, monitor and mitigate.

RAHS – BUILDING RESILIENCE IN THE FACE OF FUTURE SHOCKS

The speaker spoke on the Risk Assessment and Horizon Scanning (RAHS) program run by the Horizon Scanning Centre (HSC) in Singapore. He opined that risk management is an important component of resilience and RAHS helps agencies explore, analyze, monitor risks, and develop scenarios and strategies. He added that RAHS helps prioritize, synthesize, and identify emerging issues and risks that could have a strategic effect on Singapore.

He provided an overview of how RAHS had evolved since its inception. RAHS started off with a focus on tools and methodologies, and ultimately arrived at the current stage of developing the processes that serve as guides to the existing methods and tools. He added that RAHS had moved from the downstream process of analyzing specific issues and risks to the upstream processes of horizon scanning. As a whole, RAHS is currently at the stage of linking foresight processes for risk management.

Through the RAHS approach, HSC aims to develop an environmental scanning process and teach analysts how to explore risks by addressing the following challenges: identifying the scanning techniques, assessing the source and communicating with policymakers on emerging issues and risks. He said that the purpose of this approach was to share experiences and set RAHS as a benchmark for environmental scanning. To this end, RAHS has put together a primer for environmental scanning and provided clients with information on emerging risks in the form of customized risk reports.

He opined that the challenge of RAHS lies in translating emerging issues into visible indicators and HSC has developed a number of methods to address these needs. HSC has also developed a framework where different combinations of methods can be applied at different stages and processes of foresight strategy, which has also been made into a handbook for trainers.

He concluded by enumerating a number of important factors for the development of a futures and foresight community. First, he suggested that the younger generation should be taught about the work that had been done and they should also cultivate an intuition to think about the future. Second, collaboration with the private sector was another important factor. However, this has proven to be a big challenge and HSC is still trying to find the right collaboration model. Third, no matter how advanced the tools may be, it still cannot replace analysts. Thus, analysts should continuously develop their own area of expertise and HSC aims to gather expert analysts from diverse. Lastly, he opined that collaboration is the key to building resilience against future shocks. In this connection, events like the Global Futures Forum General Meeting serve as a good example where different parties can discuss joint projects, share open-source information and talk about emerging risks.

GIVENS AND WILD CARDS IN ENERGY FORESIGHT

The speaker delivered a presentation on how givens and wildcards influenced the way the development of the future world energy environment was viewed. He defined "givens" in this context as predetermined elements in the field of energy security that possessed a low degree of uncertainty and a high level of impact.

He stated three givens in the field of energy foresight as follows: demographics, hydrocarbon supply and climate change. He said that it was important to consider demographics in terms of energy foresight because the demographic composition of the population strongly influenced the energy ladder, namely the consumption trend of energy. With regard to hydrocarbon supply, it was a significant factor because it could not be replaced with renewable energy. However, he gave an optimistic view

that we had consumed about 1.2 trillion barrels of oil as of now, and there were still more resources that could be converted up to 9 trillion barrels of oil. He said that the problem lay in people's belief that it was not so much about how much we "have" but rather how much we "can bring to the market". Then he opined that climate change was a human-induced factor that, as a matter of fact, might be a more serious issue than simply securing oil and gas.

Lastly, he presented on the issue of wild cards, which he defined as possessing the following three characteristics: low probability, high impact and the ability to be logically accounted for after the occurrence of an event. He presented the emergence of BRINK countries, which comprised Brazil, Russia, Iraq, Nigeria and Kazakhstan, as the first wild card because these countries were capable of producing large amounts of oil. He said that Iraq was especially worthwhile to keep an eye on, because it was capable of producing oil at a low price, overload the market with cheap oil, and therefore negatively affect OPEC countries and investments in the energy market. Another wild card presented was the rise of nuclear energy. He said that unlike the traditional view, new energy technology might be able to convert nuclear energy into a potential positive wild card.

FACING UNCERTAIN FUTURE: HAVE WE LEARNED FROM PAST ECONOMIC CRISES?

The speaker presented on the 2007/2008 economic crisis, underscoring the ironic situation in which people constantly fail to prevent economic crises despite their known historical patterns. As an example, he quoted recent quantitative studies that showed that almost all economic crises followed a similar pattern. However, he said that it was interesting to note how people perceived each economic crisis differently from past crises.

He named several factors that affected people's perception of economic crises. The first factor was the magnitude of the crisis. For example, the U.S. national debt added up to USD 14 trillion, which well exceeded the entire amount of money that was spent on major projects in the United States, including the Vietnam War and the Iraq War, which amounted to approximately USD 3 trillion. In the same context, the magnitude of the U.S. financial crisis, which began in 2007, was perceived as unprecedentedly huge. The second factor was the speed at which the economic crisis unfolded. People have witnessed well-established financial institutions going bankrupt overnight, such as the collapse of Lehman Brothers in 2008.

Having acknowledged the unusual magnitude and speed of the economic crisis, he posed the questions of whether we have learnt anything from the past and whether economic catastrophes such as the credit crunch in the United States could have been forecasted and prevented. He said that regardless of certain patterns that could be derived from the series of economic crises in the past, we

still seemed to be facing an uncertain future in an uncertain world. Furthermore, the fact that financial institutions were regulated at the national level when the market was moving into an international level further complicated the situation. While acknowledging that policies and responses to address financial crises had indeed contributed to eventual stabilization and recovery, he opined that the stability that resulted from these efforts had not proven to be robust. He concluded with three reasons for this result: the inherent instability of the financial system, human beings' recurrent inability to protect themselves from the "black swans", and the Darwinian characteristic of the financial system that moves along the principle of "the survival of the fittest".

DISCUSSION

One participant asked what the weakest links in the processes of risk assessment and horizon scanning were. A speaker offered up four weak links in response: cognitive bias, the failure of organizations to network and share, deep-seated mistrust of open-source intelligence, and analysts' inherent mistrust and fear of technology.

Another participant questioned if there was a preferred profile of analysts in the intelligence community. The panel was generally in consensus that diverse expertise, backgrounds and knowledge were crucial. A speaker added the following factors that he looked for when recruiting an analyst: experience-based wisdom that could be applied when faced with new challenges, good skill of policy interactions, humility, experience with a wide range of methodologies, and a good intuition that enabled matching the right methodology to the right problem.

One participant opined that there is a difference between the concepts of "unlikely" and "uncertain", and said that people tended to make evidence and data-driven decisions whereas the future had so many uncertain factors. Given this reality, he asked how it was possible to deal with uncertainty and actual probability when addressing strategic challenges. A speaker agreed that it was wrong to pretend to know about something that is uncertain. Another speaker suggested that rather than focusing on the precision of one's forecast, the best way was to decide whether a certain event was likely or unlikely to happen and then show how confident one felt about this decision.

LUNCH KEYNOTE

The lunch keynote speaker argued for the application of resilience in mitigating security threats and crises by placing a premium on assuring that communities, corporations and countries have the capacity to withstand, respond, rapidly recover and adapt to man-made and natural disturbances. This would require developing policies and incentives that encouraged community resilience at the local level, and within and across networks and infrastructure sectors both regionally and globally. It would also require acknowledging that safety and security efforts that aimed to eliminate risks would always reach a point of diminishing returns. In most cases, a more prudent and realistic investment would be to build the skills and capabilities for managing risks.

RESILIENCE: DEFYING TERRORISM AND MITIGATING NATURAL DISASTERS

The speaker argued that the key to assuring safety and prosperity in the twenty-first century was possessing resilience in face of chronic and catastrophic risks. The years ahead would be marked by turbulence, fuelled by unconventional conflict, likely changes in climate, and the sheer complexity and interdependencies of modern systems and networks. This places a premium on assuring that communities, corporations and countries have the capacity to withstand, respond, rapidly recover and adapt to man-made and natural disturbances.

He went on to comment on the role of resilience in defying terrorism. Immediately after 9/11, the United States believed that Al-Qaeda was planning an equally, if not more, spectacular attack. However, the terrorist threat since then has been less sophisticated and on a much

smaller scale, for example, the May 2010 bomb attempt on Times Square. He noted that this was because sophisticated attacks like 9/11 required a larger group of operatives, communications with those overseeing the planning and time to conduct surveillance and rehearse the attack, which created opportunities for detection and interception by intelligence and law enforcement officials. However, smaller-scale terrorist attacks are harder to prevent and can yield a response that is costly and disruptive to the targeted society. Following from this, there is tactical and strategic value from investing in better responding to and rapidly recovering from attacks when they occur.

On the role of resilience in mitigating natural disasters and large-scale accidents, he observed that the overwhelming costs associated with disasters were often associated with the failure to prepare for them upfront. As the occurrences of disasters was inescapable, he argued that it was far more cost-effective to make an upfront investment in safeguards that mitigated risk and consequences than to pay the price for response and recovery after a foreseeable hazard manifested itself. For instance, the devastation and tremendous loss of life wrought by the January 2010 earthquake in Haiti was comparatively much larger than that experienced by Chile shortly thereafter in the face of a far more powerful earthquake.

From an economic standpoint, a society's level of resilience will increasingly be a source of its global competitiveness. He opined that the one thing that could be safely predicted with confidence is that the twenty-first century would be marked by major disruptions arising from man-made and natural threats. As such, countries that lack resilience will place themselves at a competitive disadvantage since

individuals and investors will gravitate away from places and companies that cannot demonstrate a capacity to provide continuity of essential services and operations in the face of a traumatic event.

In conclusion, given the benefits of resilience—and the direct and indirect risks associated with fragile or brittle jurisdictions and systems—it was very much in the interest of the international community to advance it at all levels. This would require developing policies and incentives that encouraged community resilience at the local level, and within and across networks and infrastructure sectors both regionally and globally. It would also require acknowledging that safety and security efforts that aimed to eliminate risks would always reach a point of diminishing returns. In most cases, a more prudent and realistic investment would be to build the skills and capabilities for managing risks.

DISCUSSION

The first question pertained to the extent of government involvement in enhancing community resilience in democratic societies. In his response, the speaker identified one of the challenges faced in the United States as the "professional protector problem". He argued that the Cold War had created in the United States a reliance on the national security apparatus to protect citizens from challenges that they themselves were able to address. This resulted in the public expectation of being protected from all forms of risks that were reinforced by the security professionals themselves, who preferred to work under a shroud of secrecy and were not forthright about the limitations of the national security apparatus. He then made the case for a "culture of resilience" that involved cultivating the public to be willing to embrace and overcome risks rather than to avoid them altogether.

A participant noted that a challenge facing governments in acknowledging risks was that it made them vulnerable to charges of overstating risks. As a result, it would be more attractive for governments to deny rather than embrace risks. The speaker was of the opinion that governments should be forthright with the public about the risk the country faced, especially the strengths and weaknesses of the policy tools to address them.

PANEL 2

RESILIENCE IN THE FACE OF FUTURE SHOCKS:
THE FIVE R'S OF RESILIENCE

The panel discussed strategies to enhance resilience. As a conceptual framework from which to approach the subject of resilience, the organizers asked to speakers to expand on the concept of the five R's of resilience which include: Robustness, Resourcefulness, Rapid recovery, Remembrance and Re-visioning the future. The presentations included the British approach to crisis management, the application of crowdsourcing for coordinating aid in the aftermath of earthquake in Haiti, an assessment of Indonesia's principle of national resilience, and the U.S.'s integrated national homeland security risk management effort. The key strategies identified included a bottom-up approach to building local community capabilities to be supplemented from the state where necessary; teamwork within and between the private and public sectors as well as at different sub-national, national and international levels; and information sharing to increase the amount of publicly available information on risks.

RESILIENCE IN THE FACE OF FUTURE SHOCKS

The speaker presented on the U.K. resilience strategy by focusing on identifying risks, risk assessment and building resilience.

Regarding the process of identifying risks, he said that it was neither possible nor desirable for the government to protect everyone against all the threats and hazards that they might face. However, it would be in the national interest to have an adequate level of national preparedness to face them. He emphasized that it was important to find an appropriate balance between building resilience at the local community level and instituting a coordinated national-level response that would necessitate government intervention. Fine-tuning such an approach, however, was difficult and would require a calculated risk management strategy. Managing consequences of risks also required a sense of shared responsibility because resilience was everybody's business.

Moving on to assessing risks, he highlighted the U.K. national risk register, which illustrated high-consequence risks facing the country. With emergency defined as any event that would cause significant harm to human welfare in the United Kingdom, the register had specific criteria by which risk was assessed. He argued that using a risk-assessment strategy was the best approach to making informed decisions for necessary policies of resilience as it enabled the U.K. government to avoid speculations and predictions of future shocks in an inherently risky landscape, prioritize risks according to the likelihood of them materializing and their impact when they do, and identify the greatest risks that would require special programs to reduce vulnerabilities, prepare for, respond to, and recover from future shocks.

When it came to building up a society's resilience, he said a whole-of-system approach was needed. He advocated a bottom-up strategy to building local community capabilities

to be supplemented from the state where necessary. He also advocated teamwork within and between the private and public sectors as well as at different sub-national, national and international levels. Sharing information to significantly increase the amount of publicly available information on risks would also help build resilience.

He concluded by stressing the importance of building a resilient national infrastructure and improving the capability and capacity of local respondents as well as the generic response capability at the national level.

CROWDSOURCING THROUGH CRISIS: EVIDENCE OF ADAPTABILITY AND RESILIENCE

The second speaker spoke about crisis mapping using the crowdsourcing framework with a focus on the resourcefulness and adaptability of local and external actors in a crisis situation.

She underscored the extent to which we live in an age of complex disasters with threats coming from all directions. Disasters, such as those emanating from extreme weather, were not isolated incidents but evident worldwide. Moreover, local threats could internationalize and reverberate across the globe and tended to toggle between extremes (drought, floods and earthquakes) with disproportionate effects.

Complex disasters required complex disaster responses. Using an "expired-tired-wired" paradigm to highlight current trends, she then showed not only the changing nature of threats facing us but also the transforming prism from which we view our environment. She said that the world was moving from a closed system of traditional defense to a complex, adaptive system through a networked, multi-actor approach. Web technology and mobile phone applications were all challenging traditionally understood boundaries of roles in crisis response. Today, in times of crisis, mobile phone users would snap pictures, record videos and text information regarding the emergency long before the first responders even arrive. Furthermore, the global media would widely disseminate such images and information, almost immediately engaging the national audience. Moreover, Web 2.0 was providing the collaborative platform for individuals from different segments of society to come together.

She defined crowdsourcing as the outsourcing of a task to a crowd through platforms such as those provided by Web 2.0. It was a way of communicating a problem to a community that could then work on the issue either autonomously or collaboratively. Different tools of information—from news broadcast to SMS, e-mails, blogs, Facebook and Twitter—would provide the data that could be aggregated and put to a map. As a concrete example of crowdsourcing at work, she showcased "Ushahidi", a program created in 2008 in the midst of political violence in Kenya. Used as a platform for citizens to send text messages and e-mails, the mapping software aggregated data and helped visualize what was happening on the ground almost in real time, from mapping ongoing violence to providing information on safe havens. She also showcased how crowdsourcing was utilized after the Haiti earthquake. The tragedy saw a whole stream of people volunteering information through satellite imagery, through Google as well as through the U.S. government, to in fact create a multi-sector, multi-actor partnership between the emergency services, the Haitian telecommunications, the U.S. government and Ushahidi. Just days after the earthquake, she noted that the group had quite quickly organized and represented a complex, adaptive system that was receiving and processing volunteer information, much of which came from outside Haiti. Such interactive mapping of the crisis terrain reflected an ecosystem of organic support that aided the visualization of a crisis so as to expedite recovery.

There were numerous advantages of crowdsourcing. The trend tended to demonstrate the innate resourcefulness of people, especially with the technology at hand. Such a whole-of-society approach leveraged different access points and ultimately illustrated global assets—instead of deficiencies—that could be built on. However, crowdsourcing had its limitations too. With information flooding in, the quality of data needed to be constantly monitored. Information could often also be duplicates so it was important to be able to effectively organize data. Further, strong leadership was necessary and there must be a willingness to share information. That said, crisis mapping would continue to be a vital component of crisis management.

INDONESIA'S APPROACH TO RESILIENCE

The speaker presented on Indonesia's approach to resilience. He argued that the country possessed a culture that supported both whole-of-government and whole-of-society approaches towards resilience. The concept of ketahanan nasional (national resilience) had been ingrained in the national psyche largely because of non-stop challenges facing the country from within and without. He also argued that Indonesian resilience in actuality stemmed from the country's inherent weaknesses rather than its strengths.

He explained some of the factors that had helped shape Indonesia's approach to resilience. For one, Indonesia had a long and painful colonial past. It also had a difficult start at nation building, with its complex ethno-religious make-up. Sporadic inter-province wars further weakened national cohesion at all levels. Non-stop internal threats—a phenomenon still evident today—made Indonesia susceptible to crumbling from within. In addition, Indonesia also faced various challenges from outside, for example, external actors during the Cold War often played on its internal weaknesses. A poorly performing economy and poverty on the streets further mired the country.

He believed that Indonesia's leaders played an important role in shaping national resilience. Strong leadership, however, could be a double-edged sword: on the one hand, there was a clear national commitment to national resilience but on the other hand, strong personalities often lend to a weakening of institutions. Sukarno's role, for instance, in spearheading the notion of one people, one nation and one language helped Indonesia internalize the spirit (semangat) of unity and nationalism but despite such a powerful source of national strength, the Indonesian state and society remained weak. Yet, the notion of a Great Indonesia stemming from its grand imperial past continued to give Indonesian leaders a sense of regional leadership entitlement. He argued that it was the very frustration in knowing that such greatness cannot be re-captured that made Indonesia's leaders push forward all new ideas to ensure a resilient nation. This resilience had even been integrated into the larger Indonesian political structure, including Pancasila. This was how a weakness was converted into a source of strength.

He then noted the nexus between security and resilience, and cautioned against attempts to separate the two in Indonesia, largely because the main security threat facing the country was internally derived. That said, for a country so diverse, Indonesia's main defense against an external attack was inadvertently its steadfast national cohesiveness.

In today's democratic Indonesia, resilience remains very much a part of the national psyche. Resilience, in fact, had arguably strengthened because it shifted from a whole-of-government to a whole-of-society approach. Moreover, instead of being securitized by the military, civilians are in command. He concluded that Indonesia aimed to develop an instinct regarding how resilience could be effectively mined as a source of national strength. Although Indonesia had come a long way, it still had a long way to go.

BUILDING RESILIENCE THROUGH RISK MANAGEMENT

The speaker spoke about a complex array of risks facing societies today and addressed the question of how nations should prepare for more resilient communities. Specifically, she spoke about an approach taken at the U.S. Department of Homeland Security for enhancing the country's safety, security and resilience through an integrated national homeland security risk management effort.

She noted that the new homeland security framework did not involve a complex restructuring of the department or flashy new programs. Rather, the starting point was based on the idea of interconnectedness and mutual responsibility. This included building bigger and stronger security teams that would include all citizens—local communities, first responders, community groups, business groups and law enforcement—by employing the notion that homeland security began with hometown security. Security against evolving threats should be a collective endeavor because success required the strengthening of

partnerships with the wider society and a focus on values like resilience and shared responsibility. Drawing on the traditions of civil defense, she said that people should have a sense of being more responsible for themselves.

She then argued that risk management formed the base of resilience. Risk management analyses allowed agencies to prioritize hazards and the manner to address them. Homeland security was ultimately about effectively managing risks to a nation's security by building a foundation of insurance, security and resilience, as well as facilitating the normal everyday activities of society. She also emphasized how an integrated risk management strategy would lead to resilience across enterprise, an interconnectivity that was especially vital in the United States where there were over 87,000 units of local governments on top of the individual police, fire and emergency management departments.

She also highlighted the range of threats and long-term global challenges facing the United States through a national homeland security risk assessment. Such assessments helped to identify homeland security risks as well as alternative approaches to managing those risks. For example, she highlighted the recently completed RAPID (Risk Assessment Process for Informed Decision-Making), an all-hazard quantitative assessment of risk that allowed decision makers to assess the uncertainty inherent in a wide range of hazards. The program also allowed decision makers to identify the best opportunities to reduce risks and impact of hazards.

DISCUSSION

A participant questioned the panel how risk management could be implemented at the national level if there was no local capability to deal with risk, and also how the government could ensure that there was capacity at the local level to respond to crises. In response, a speaker argued that more impact-based planning was needed over scenario-based ones. Another speaker concurred, adding that the government should also do what it could to communicate its role and function during particular crises at the national level. And with regard to building local-level capacity, she suggested the provision of federal grants to get initiatives started and also encouraged programs that included a community resilient registry to develop local resilient profiles. Referring to emergencies other than natural disasters, a speaker highlighted the apparent disjunction between the local and the national in Indonesia when a terrorist cell was uncovered earlier this year in Aceh. He said local intelligence was what had led to the terrorists while the response at the national level lagged. He argued that it was important to work in sync since "draining the swamps" would have to come from locals.

Another participant questioned the validity of an approach to resilience that at times seemed more bureaucratic than substantial. Highlighting the whole-of-society approach,

the participant then asked how governments could encourage societies to be active in times of crises. A speaker responded that in times of crisis people generally tended to want to act purposefully and, while doing so, people would take on different roles—some were organizers, some leaders—and these were roles that they would, in most other aspects of their lives, naturally identify with. She argued that an innate spur to action, a desire to help and the personal capability to do so largely tend to already exist and that it was state institutions that needed to enhance their capability to respond.

A participant asked who would decide when and how a local incident would require national attention. For instance, in the tragedy of Katrina, the participant argued that if the hurricane had struck outside the United States, the U.S. response would have been faster and more coherent because it would have resulted in a direct command-and-control response from the military as well as from NGOs and aid organizations that would have dispensed with local state politics and complex bureaucracy. In response, a speaker said that the U.S. political structure was really its strength as well as a challenge when it came to dealing with such major tasks. The United States would handle such emergencies by building a better team that—while not demonstrated during Katrina—had been put in practice a lot since. Another speaker noted that there was indeed a need to more clearly identify the various local and state responsibilities. Another speaker added that the ultimate aim of crisis response was long-term recovery and getting communities back to their feet and not merely about the immediate response. He said that there were often instances of how immediate responses to crises could confound recovery. For example, many localities often used schools as shelters for displaced populations in the immediate aftermath of disasters but if schools could not reopen quickly, children could not go back to the classrooms and parents could not go back to work. This would be an obstacle to the community getting back on its feet.

To a query regarding how the U.K. fuel emergency was being conducted, a speaker explained that the United Kingdom had learnt many lessons from three types of emergencies: the fuel strike, the flood emergency and the foot-and-mouth disease outbreak. These incidents demonstrated how difficult it was to elevate issues that were initially local but very soon needed a coordinated initiative at the national level.

A participant commented that the more the United States invested in security, the less tolerance there was for failure. A speaker agreed, saying that when more resources were diverted and pumped into security programs, people expected perfection. She said that the U.S. government lacked serious and honest dialogue to emphasize resilience and shared responsibility for security with the American people, unlike during the Cold War. She was of the opinion that the idea of risk should be boiled down to its simplest: as something bad that could happen and as a decision of consequence that everybody would make on a daily basis, like getting into their cars. Perfect protection simply could not be assured. Another speaker added by cautioning governments against over-selling their risk management tools because there would be a backlash if they were to fail. He said that risk-management tools that could not survive "the morning after" threats put governments at risk of system-wide failure because they would lose credibility. In no small part was resilience about assuring the people and instilling confidence in them if and when things go awry.

Commenting that part of resilience was about a capacity to coordinate response, a participant asked how far resilience strategies focused on encouraging a greater understanding that weak links of a chain existed. In response, a speaker said that as societies developed and grew, public dialogues would become increasingly taken for granted. Hence such conversations should be institutionalized at the strategic level.

THE GFF DISCUSSION: "GFF NEW DIRECTIONS"

Two speakers provided a general introduction of the GFF and its future plans, namely what the GFF was about, the evolution of the GFF, future activities of the GFF and the function of the GFF website.

GFF NEW DIRECTIONS

On what the GFF was about, the first speaker described the GFF as a loose association of countries that aspired to fill the gaps that existed within their security apparatus. The purpose of the GFF was to better understand the medium-to long-term transnational and national security issues. He identified three requirements that countries should meet as GFF members: an interest in foresight, contribution to creating a platform for joint-research and collaboration,

and be open to the exchange of practices among security intelligence services. He said that the GFF operated on a decentralized structure and also served as an exemplary international collaboration between both government and non-government participants.

On to the evolution of the GFF, he stated that the GFF was founded at an international conference in Rome in 2004 that was jointly organized between the U.S. and Italian governments. Having been one of the largest multilateral gatherings that dealt with security and hazard assessment, it derived an agreement for a formal flexible network that linked different countries together for a common cause. Subsequently, this led to the first GFF full-membership meeting in Washington in 2005, which led on to a series of collaborative workshops and conferences until the present.

The second speaker presented on the current activities and proposed plans of individual GFF Communities of Interest (COI) for 2011. The Radicalization and Counter-Terrorism COI planned to focus on home-grown terrorism and tools for forecasting individual and group aggression towards violence. It would look into the impact of social forces, for example, education and community leadership, as well as the utility of various analytic tools that could be found in the open-source domain. The Illicit Trafficking COI would focus on the medium- and long-term impact of various driving forces of globalization on illicit trafficking as well as the reciprocal impact of the patterns of illicit trafficking on social and political stability. As for the Proliferation COI, the Swedish government would assume its leadership, focus on best practices and lessons learnt from previous experiences, and draw on topics previously identified in the GFF to develop innovative tools to counter proliferation. The Human and Natural Resources COI aimed to form a cross-disciplinary community to develop an integrated perspective to better understand the interactions between diverse human and natural resources security issues. The Emerging and Disruptive Technologies COI aimed to better understand the implications of new science and technologies on global security while focusing on cyber security through a series of workshops and collaboration with other COIs in the present. The Practice and Organization of Intelligence COI had initially focused on analytic training,

organizational change and performance management techniques, and now sought to further address the issue of analytic collaboration between different agencies and the use of online technologies. Lastly, the Strategic Foresight and Warning COI was planning to hold a conference at the end of 2010 to discuss which methodologies could translate longer-term foresight in such a way that was useful for policymakers. In addition, it would continue to focus on linking foresight and resilience and also on selected substantive issues that did not fall into the areas of other COIs.

In closing, he gave a general overview of the GFF website and re-emphasized its importance as a cost- and time-efficient platform for international collaboration. He opined that the GFF website was currently not being used as actively as it should and gave a number of suggestions to overcome this problem: (i) have a group of leading academic thinkers visit the website and post comments and questions, (ii) make the website more user-friendly, and (iii) grant more website members the ability to post readings and comments on the website. He stressed that the GFF was not a centrally directed organization but rather a platform for various participants to interact and thus, contribution to collaboration and dialogue by all GFF members were crucial.

FUTURES THINKING IN THE SINGAPORE GOVERNMENT

The panel consisted of representatives from various ministries sharing their approach of infusing futures thinking into strategic planning. This included exploring cross-cutting issues, experimentation and discovery, establishing inter-agency networks, and developing resilience through risk governance. Some challenges faced when thinking about and preparing for the future were differentiating between weak signals and noise, establishing clear divisional responsibilities to facilitate focus and operational efficiency within and between agencies, and converting weak signals into actionable insights for policy formulation. Solutions to these problems include building and updating methodological toolkits by tapping into a wider network of foresight practitioners in Singapore and beyond, strengthening relationship with the private sector on top of improving inter-governmental networks, and effectively translating ideas into actionable policy prescriptions.

FUTURES THINKING FOR NATIONAL RESILIENCE – SINGAPORE'S CENTRE FOR STRATEGIC FUTURES

The speaker presented on futures thinking for Singapore's national resilience and the work of the Centre for Strategic Futures. He explained that the centre utilized existing

scenario-planning methodology complemented by Risk Assessment and Horizon Scanning (RAHS), a program that has helped canvass large amounts of open data to detect weak signals of strategic shocks and discontinuous change. The centre has focused on three particular areas: (i) experimentation and discovery, (ii) networks, and (iii) resilience through risk governance. These in sum provided for a holistic governance architecture for change management.

With regard to the centre's first focus on experimentation and discovery, he explained that, because complex modern problems meant no clear patterns of cause-and-effect could be easily discerned, a management-by-discovery process involving learning by doing was needed. Such an approach would be much unlike management-by-design, a more structured program of planning that policymakers were more used to. Moreover, he said it was important to develop a safe-fail culture (versus fail-safe) where failures could to be looked at as learning experiences, not incidents that invite retribution.

Moving on to the centre's second focus on networks, he pointed out that no individual agency had the ability to come up with all the answers to today's multi-dimensional

problems. Harnessing a platform for diverse networks both within and without the government could therefore help. Local think tanks and business communities as well as international networks like the Global Futures Forum could also be tapped to identify potential black swans.

The centre also worked to promote resilience through risk governance, its third focus. He said that it was hoped that the centre would develop into a place where there could be jockeying of ideas and trading of different perspectives. Also, a system of governance that was more akin to spider silk—flexible yet strong—was preferred over a cathedral-like structure that was strong but if destroyed would lead to a lot of collateral damage and would need a long time to be reconstructed.

LEARNING BY DISCOVERY

The speaker shared the workings of the futures unit in the Ministry of Community, Youth and Sports, Singapore. He explained that even though the unit largely concerned itself with social policies in Singapore, it was important to be aware of how the economy could impact them, just as finance ministries would conversely pay attention to the long-run social impact on fiscal policies.

He explained that part of the work at the unit included envisioning how Singaporean society would look in 2025. He said that minute changes in details when summed up would have a critical-mass effect, which was why it was important to look at a system in its entirety to begin to understand how a society could dramatically change over time.

He highlighted some of the projects the unit had worked on and then moved on to demonstrate the social impact of Singapore's ageing population as an example of the practical applications of the meeting of social changes in the long run. He said that Singapore's existing model of economic sustainability and its labor force profile could not support the current level of affluence and growth that Singaporeans had grown accustomed to. So it would be good to change assumptions and switch mental modes from accommodation to adaptation. He explained that if Singaporeans lived longer, they should then ask what they

could do to continue making themselves economically relevant for longer. Such an approach would serve national interests and increase self-reliance.

As a further example, he demonstrated how families in Singapore constituted the nucleus around which the government would base its social policies. But now with fewer and later marriages and smaller families, current social policies have become questionable, especially when juxtaposed against possible economic crises over time. He explained that futures projection could help the government reinterpret how to make different decisions to avoid potential undesirable futures.

He concluded by sharing some of the lessons the futures unit had learnt thus far. First of all, futures thinking required senior management support because it needed resources. Second, selecting the right kind of people for the job was important. Third, futures practitioners had to learn by doing and undertake projects suited for the context and culture as well as the client base. Also, a healthy belief in the self was important because the nature of futures work meant that practitioners could be wrong most of the time.

DEVELOPING STRATEGIC FORESIGHT AT MTI

The speaker shared with the audience why and how an economic agency such as the Ministry of Trade and Industry in Singapore set up a dedicated futures unit. She detailed three major challenges the ministry faced when thinking about and preparing for the future: anticipating, networking and translating.

The first challenge of anticipation involved capitalizing on complexity and discerning important but weak signals in the present amidst all the noise. The futures group had to balance the forward-looking nature of research with practical implications. Although research that was too far out into the future would be too removed from reality and would not gain traction, being too pragmatic could mean losing the ability to see blind spots and detect potentially disruptive trends. The futures group would thus play the role of a scout by looking for anticipated events just over the horizon as well as trying to catch trends that might fall through the gaps.

The second challenge of networking across divisions involved having clear divisional responsibilities to facilitate focus and operational efficiency while working well together with other teams and departments. The futures group had to effectively leverage and connect with other sources because they served as platforms to receive ideas, share research findings and collaborate on projects.

The third challenge involved translating ideas by turning weak signals into actionable insights that might impact policy formulation. Ideas generated needed time to gestate, mature and develop into insights and strategy but, considering the fast-paced global economy, many issues were highly time-sensitive.

She elucidated that the three challenges could be reframed into questions such as: Which emerging trends could be relevant for Singapore's economic future? How could weak signals be better spotted and understood in order to judge their potential effects on the government's goal of future economic growth, job creation and higher standards of living? Such far-sighted questions remained in the background as the futures group worked to identify nascent and emerging trends that might have significant bearings on the mid- to long-term economy of Singapore. The group also needed to churn data into insights that could help inform policy developments as well as tweak and complement policies and recommendations, and catalyze new areas of focus. Inadvertently, the group dealt with wide-ranging issues because many things could impact Singapore's economy, including science and technology, emerging economies, and societal and environmental issues.

The futures group saw building futures capabilities as a continuing process; some of the lessons it had learnt along the way included building and updating their methodological toolkit by tapping into a wider network of foresight practitioners in Singapore and beyond, strengthening relationship with the private sector on top of improving inter-governmental networks, and effectively translating ideas into meaningful insights.

DISCUSSION

A participant asked if the various futures groups used risk methodologies in their work. A speaker responded that the idea of risk governance was a necessary complement to the more analytical aspect of foresight and futures because without it, the latter two would just remain esoteric. Hence it was important for futures work to be relevant to policymakers. Another speaker added that risk should be regarded as the other side of the coin to opportunity. So having to identify opportunities also meant having to be aware of risks. Another speaker added that with regard to social policies, risk is a loaded term with negative connotations. Hence it would be better to communicate the concept of risk using the vocabulary of the clients.

A participant asked for the foreign policy implications of a video on China screened during presentations. A speaker responded to say that the video was generated for the economic community, not for the purposes of foreign policy. Another speaker added that the video was an excellent example of the curatorial role of the futures group because it helped spark discussions and debates.

THE PRACTICE AND ORGANIZATION OF INTELLIGENCE/ RADICALIZATION AND COUNTERTERRORISM: ADDRESSING EMERGING FORMS OF TERRORISM

The panel examined emerging forms of terrorism and the strategies by the intelligence communities in addressing them. Two trends identified were the radicalization of inmates in Canadian prisons and Islamist extremism and radicalization in Canada. Other presentations included a review of the work of the radicalization and counterterrorism community of interest, and an assessment of the threat of online radicalization.

COUNTERTERRORISM METHODOLOGIES TO SUPPORT THE PROFESSIONAL REQUIREMENTS OF THE ANALYTICAL COMMUNITY

The speaker spoke on the topic of counter-terrorism methodologies to assist the analytical community in anticipating new threats and terrorist groups. He began by discussing two previous GFF conferences on counter-terrorism and radicalization that took place in June 2010. The findings of these conferences suggested that the GFF should begin to explore analytical methodologies and tools that could be used to anticipate future threats and terrorist groups. He proposed that over the next year, the COI on radicalization and counter-terrorism should work to identify open-source methodologies and tools developed by academia and industry and which had the potential to make a difference in improving understanding in the analytical community. The objective, he said, would be to help analysts keep ahead of the continuously evolving terrorist threat.

The new research agenda he described was meant to be practical in its application and would be used by analysts in their tracking of terrorism globally and locally. This, the speaker offered, was intended to mitigate the problem facing intelligence communities world-wide of being too focused on current threat developments, on a day-to-day basis, that they might miss recognizing gradual subtle changes, thereby failing to stay ahead of them operationally.

He said that analytical methodologies and tools to be examined in the coming year would focus on enhancing capabilities in the following six areas: root causes of terrorism conflicts, radicalization of violent extremism and terrorism, recruitment and organization of terrorist groups, terrorist group geographical areas of operations and location of terrorist incidents, forecasting the emergence of new types of terrorist groups and their likely future warfare methods, and measuring the effectiveness of governmental responses to terrorism.

In conclusion, he proposed that the way to move this research agenda forward would be to create a steering committee made up of GFF members to oversee a small team of analysts and practitioners conducting requirements and needs analysis in order to prioritize areas needed to be covered. Once these areas were identified, methodologies and tools would be selected to best address these areas of need. This would be followed by an expert's workshop for the findings to be presented and reviewed with a final report of these findings disseminated to the larger GFF community.

RADICALIZATION IN CANADIAN PRISONS

The speaker spoke on the issue of radicalization in prisons in the Canadian context. While the issue of radicalization in prisons was now widely recognized as an area of concern, this had only been of interest to intelligence communities over the past two to three years. She shared that three years ago the government of Canada began assessing the phenomenon of radicalization in prisons in this country. However, at the time, due to insufficient information, the assessment was unable to ascertain the extent of the threat to national security that radicalization in Canada's prisons posed. The report did nonetheless identify three key emerging areas of concern. First, inmates were responsible for converting other inmates to a radical interpretation of Islam via an established system of recruitment and indoctrination that utilized official Islamic prayer services in prison. Second, conversions to radical Islam were more likely to occur in prisons that did not have contracted imams. Third, members of the general public with a radicalized interpretation of Islam had been found, in some cases, to take advantage of Canada's prison visitation and volunteer programs in order to gain access to inmates and spread their radical views.

The speaker went on to say that Canada was in the process of updating its assessment, examining whether or not the threat of radicalization to Canadian national security had evolved. This new report utilized a questionnaire that was distributed to a random sample of prison correctional staff across Canada. In addition to these questionnaire responses, the assessing organization also obtained correctional intelligence reports that covered the period of review. Further to this, Canada's security and intelligence community had steadily allocated more resources to study this topic. These different sources of information combined had enabled the assessing body to ascertain more accurately the level of radicalization in Canadian prisons.

Canadian correctional authorities were adjusting to the fact that they now had inmates convicted of terrorism in their prison populations, a reality that created new problems concerning prison radicalization. The findings of the new report suggested that there had been an increase of inmate-on-inmate recruitment to radical Islam in Canada's prison population over the past three years. However, the precise number of inmates who had made such a conversion was at present unknown. For the most part, the occurrences of Islamist radicalization identified since 2007 were assessed as isolated, meaning that they had developed independently of one another, with no indication that these converts had any association with known international terrorist organizations like Al-Qaeda.

In conclusion, the speaker indicated that the findings of the most recent report had shown that the number of imams contracted by the government of Canada to provide Islamic services had continued to increase, thereby addressing one of the findings of the initial report on prison radicalization. However, there were still cases of inmates within the system providing services on their own, a continued point of concern. The presenter went on to say that there were also cases of new converts being introduced to convicted terrorists in prison, which would require monitoring. Also, a new finding of the report cited the recent phenomenon of radical Islam influencing prison gangs, which was an area believed needed to be further investigated.

ISLAMIST EXTREMISM, RADICALIZATION AND CANADA

The speaker addressed the issue of Islamist extremism and radicalization in Canada. He categorized the state of radicalization in Canada as being roughly where the United Kingdom was in 2003 but indicated that Canada was catching up quickly. He went on to say that Canada,

like most Western countries, was facing a growing concern over violent Islamist radicalization and extremism and, as such, its efforts to identify and counter it were growing concurrently. Some of these efforts focused on a better understanding of the nature of violent Islamist extremism in Canada while others involved enhancing efforts both in Canada and overseas to counter it, an effort which involved many government departments.

In discussing the evolving threat of terrorism in his country, the speaker said that Canada was becoming a target. He identified four areas of focus for Canadian authorities: second generation Canadians, converts, spiritual leaders and militant training. In terms of radicalization, the appeal of radicalism was being examined, as was the role of the recruiter in this process. Spiritual leaders, the role of imams in mosques and the role of Internet inspiration were also issues that the government was exploring. On the issue of training, the return to Canada of those who participated in Afghan was of grave concern and was being watched closely.

Radicalization associated with Sunni Islamist extremism was also of great concern to Canada. He pointed to a growing number of indicators of violent extremism having come to light, one of which was Canada's role in the war in Afghanistan, which had been pointed to as a key driver in turning some individuals to radicalization. However, the speaker noted that the radicalization process was one with no specific profile in place and where a variety of factors and drivers exist in all forms.

The speaker then went on to discuss how counter-radicalization efforts in Canada focused on the understanding of the context and grievances of individuals being radicalized. There is specific attention being paid to communities of interest, where the government is working on early identification for prevention. During this examination of radicalization, the government had come to recognize the need to identify charismatic leaders within ethno-cultural communities. The government was interested in identifying these individuals who were likely to serve as radicalizers, but also to identify individuals who might be able to counter radicalization. This is being done from a multi-agency, multifaceted approach that seeks to consult international partners in order to better understand common experiences.

The speaker concluded that it is important for the security and intelligence community to anticipate future trends in radicalization and recruitment techniques by identifying grievances emerging in one country or region that could subsequently emerge in others. He also suggested

that examining radicalization from a cross-cultural or cross-group perspective would help in the collective understanding of the phenomenon.

ONLINE JIHAD AND THE ISSUE OF INTERNET RADICALIZATION

The speaker spoke on the topic of online jihad in Indonesia and the issue of Internet radicalization. She began by discussing the world of online Indonesia where there were approximately 30 million users accessing the web, a number that accounted for approximately ten per cent of the population and was expected to grow in the coming years. She cited a number of Internet sites in Indonesia that supported terrorism and extremism and offered access to forums where likeminded individuals could gather and share their ideas. Group statements, martyrdom videos and bomb making manuals could all be found on these sites, which were fully translated to the Indonesian and Malay languages. She also pointed to websites as places where fatwas could be found and that these extremist sites also offered venues for donation to the "cause".

While she felt it important to highlight the presence of extremist websites in cyberspace and what they offered, she also felt it necessary to take a step back and question the ease with which the Internet was able to radicalize new recruits. She went on to discount the often bandied-about theory that the Internet acted as a sole source of radicalization and instead proffered that the Internet offered those who were already predisposed to such thinking a place where they were able to confirm their already pre-established beliefs. She based this assertion on her interviews with numerous detained terrorists who explained that while they might have indeed used these radical websites, they used them as places to find fatwas to legitimize their operations. She asserted that the root of the problem rested in the real world as opposed to cyberspace. She went on to point to some of the real world drivers of radicalization in Indonesia today, which included family ties, teacher-disciple relationships and the concept of

the larger brotherhood. She clarified that the individuals spurred on in their radicalization towards violence could be motivated by any number of factors running the gamut of following: family "tradition", finding meaning in life, looking for adventure and atoning for past sins.

She concluded her talk with a number of points. First, she cited that as of now there was no accurate or effective measure in place to gauge when, or if, the level of online participation of radical websites actually spurred an individual to move toward violence. She also offered that it was difficult to define what "extremist" websites were and that this difficulty stemmed from the fact that different contexts and different experiences made it next to impossible to categorize across the board.

DISCUSSION

A member of the audience asked whether highly publicized disruptions of terrorist plots worked to deter extremism or such disruptions served as examples for other extremists to follow instead. A speaker responded that high-profile disruptions were a double-edged sword and could result in both of the outcomes mentioned in the question. Another speaker also replied that highly publicized crackdowns did not help to warn off terrorists and did not thwart their efforts. To this, a member of the audience responded that high-profile disruptions had been of great help in garnering public support, particularly after terrorists were put on trial, which helped open the public's eyes to the threat of terrorism in their country.

A final question from the audience was on the lack of a systematic framework for across-the-board analysis. To this, a speaker responded that it was a difficulty and that the community was working towards systemizing analysis in this regard. Another speaker followed up by saying that getting anything of meaning out of radicalization research required keeping things in context and avoiding conflating different kinds of terrorism.

LAUNCHING OF THE HUMAN AND NATURAL-RESOURCE SECURITY COI

The panel addressed new trends in human and natural resource security and how to address them. The challenges identified by the speakers were the consequences of environmental changes and the inadequacy of current physical and legal frameworks in addressing them, the challenges to a low carbon energy future, and the security threats posed by infectious diseases. A case was made for the development of a strategic framework to address these various risks based on the concept of "human security" that was people-centric rather than exclusively focused on securing the sovereignty of the state.

FROM CONSTRAINTS TO VARIABLES: FACTORING ENVIRONMENTAL CHANGE INTO SECURITY

The speaker began her presentation by highlighting that much of the world's physical and legal infrastructure was designed for environmental conditions that existed at the time when it was planned. Using energy infrastructure as a case study, she showed that it was no longer sufficient to focus on how people affected the environment. For real security, it was necessary to examine how a changing environment would affect people.

She discussed how the term "climate change" limited the discussion while "environmental change", which considered a lot more factors, was more appropriate when analyzing a disruption. She illustrated this point by drawing attention to physical installations. Much of the defense capabilities of cities were based on the assumption that the environment they faced at the time they were built would not change, which was simply not the case. The environment was already changing—and in very dramatic ways—and climate change was not the only reason this change in the environment was happening.

Looking at some of the energy infrastructure case studies and impacts, it was noted that global energy systems were going to be seriously affected by environmental change, which, in turn, undermined security in many different ways. For instance, a key hub like the U.S. Gulf Coast going down due to Hurricane Katrina could result in a spike in global oil prices and affect everyone. A lot of oil and gas infrastructure were found in coastal locations like Singapore, and were vulnerable to sea level rises, storm surges and changing storm activity.

She spoke about how installations linked to water energy infrastructure were now facing two sets of problems: they were having problems generating energy and with the actual site stability. The same challenges applied to nuclear energy infrastructure, which required an enormous amount of water for cooling, and were usually located along the coast where site stability could be an issue with an ever-changing coastline. Furthermore, in hot summers, many nuclear reactors had to power down, or shut off, because they were overheating. Renewable energy infrastructures were also not immune. Hence, if the focus were solely on the impact of people on the environment and not a changing environment's impact on people, an analysis of the vulnerability of the systems in place would be incomplete.

Another issue to consider was the role of legislation in undermining resilience. There were many pieces of legislation embedded throughout the entire system that did not take environmental change into account and did not take existing environmental realities into consideration. This, in turn, undermined security.

Implicit in current legislations was the assumption that there would not be changes in the surrounding environment and that coastlines were not going to retreat. But, as the speaker pointed out, since coastlines were retreating, there might be implications for exclusive economic zones. In the case of the Arctic, the focus was on water but the major problem was land. The permafrost was thawing and thus undermining infrastructure, especially energy infrastructure. This may lead to an increase in shipping off the Russian coast, which would dovetail very well with Chinese interests in the Arctic. The Chinese were very active in the Arctic. They already had research bases in the Arctic and Antarctic, an icebreaker, observer status on the Arctic Council, and large number of Chinese nationals working in Siberia. The Chinese were also actively courting Canadian aboriginal leaders and this was where domestic security concerns for many of the Arctic areas arose. The relations between China and the Canadian aboriginal leaders were sub-lateral—not bilateral—as it would be very difficult for the Canadian government to redirect the way that it was potentially going. In sum, an analysis on the Arctic that did not include environmental change issues would be an incomplete analysis.

THE NEW LOW CARBON ENERGY FUTURE – SYSTEMIC CHALLENGES AND VULNERABILITIES

The speaker shared that, with the changing landscape of energy priorities towards a new low-carbon economy, the old challenges of security and risk management would be deluged. This involved a new set of very complex interactions between political, economic, environmental, technical and cultural perspectives. He outlined some of the less considered aspects of the new energy world order.

Assessing attempts made to move towards a low carbon future, he noted that in energy, there was a defined future especially for one area of infrastructure—more of our energy was going to be delivered to us by grids at the end of 2100. However, one of the major challenges was that most of the infrastructure currently on the ground was aging. This meant that all infrastructure in the Western environment needed to be replaced over the next 40 years, and governments were placing large amounts of funding into kick-starting that activity. The problem was that the cost of replacement was extremely high. The traditional grid might be slowed down by challenges like natural as well as man-made events. However, cultural issues were the biggest barriers moving forward, particularly when there was a lack of cultural acceptance of these activities.

There were two different groups with some control over the way the world operated: state-directed groups and free-market groups. There was a race going on between the two at the moment in terms of delivery of smart infrastructure. Free markets were not good for driving down costs and getting the best economical deal. State-directed activity was faster at responding to change. For instance, getting three million people to make a dam was not a problem. In a free market, it would involve 10 years of consultation. Even then, the results might not be the ones sought after. However, he pointed out that one interesting aspect now was that the financing of the smart grid in the West, run by a free-market group, was actually coming from investments mainly from state sovereign funds.

Focusing on the free-market delivery aspects, he argued that the problem with regulated markets is that they take a long time for the legislation to actually catch up with some of the aspirations, of which technology could already deliver. The other aspect related to energy infrastructures is the high barrier to market entry for innovation and new players. From a resilience point of view, he argued that smart infrastructure requires a new mindset—politically, economically, technically, environmentally and culturally—to be able to deliver a secure environment. The inability to achieve any one of these would result in system-related problems.

The speaker ended on the fact that the smart grid low-carbon development was being driven at the moment by many different aspects that were not under the control of any single entity in the market place. The West expected to get a huge range of benefits out of these developments but he believed that state-directed activity would probably deliver it before free markets got there.

SECURITY IMPLICATIONS OF HEALTH EVENTS

The speaker noted in her presentation that health events such as infectious disease pandemics and toxic industrial chemical exposures directly impacted national and international security interests. Moreover, natural disasters and humanitarian events frequently manifest their largest impact on the health of local populations, with subsequent political, military, economic and social upheavals. Longer-term issues such as the aging of populations, climate change and population movement would impact health either directly or indirectly, and should be considered in the security calculus of both developed and developing nations. Furthermore, potential health outcomes should be considered in policy decisions for a wide range of non-health security issues.

The speaker shared that health events were internationally defined as that of public health emergencies of international concern, and these included all hazards (such as biological, chemical, radiological and nuclear hazards, regardless of intent) and not just infectious diseases. Some of the drivers of pandemics included globalization, travel, migration, the interface between animals and humans, and the agricultural security, environmental security and human security interface.

It was pointed out that pandemics presented health and infrastructure impacts, widespread absenteeism, and overwhelmed the health infrastructure. Pandemics could also bring about third-order impacts like the firing of ministers during SARS and government fallout during H1N1 over the transiting of military personnel through countries, particularly those from the United States. Another third-order impact was the agricultural backlash that followed the swine influenza outbreak, where swine was slaughtered even though it was no longer the source of the pandemic, as the virus had already adapted to humans.

Besides pandemics and new viruses, there was a re-emergence of existing diseases like malaria and tuberculosis. It was highlighted in this case the intersection between environmental security and health security, remarking that a decline in the use of DDT to control insect was what led to malaria re-emerging in many countries. She also added that the crowding of people was an issue as this could potentially help spread infectious diseases.

Looking at how environmental disasters had an impact on health, she argued that there was a need for awareness on the intersection between health, environment and insurgency. Floods in Pakistan had seen not just the international community responding but the Taliban as well. Other nefarious actors such as the Hezbollah were also using health and education to gain legitimacy as a government entity.

She concluded that an assessment of the social, economic, military and political implications of health events as well as the factors either competing with, or influenced by, the health landscape was needed. Health events, as she reiterated, were security issues. She also spoke of the need to develop "integrated thought", as integrated health and security information would strengthen warning and forecast capabilities. Engaging the health community would enable health as well as security officers to see health events as security issues and to understand the second- and third-order impacts of such events.

THE "HUMAN SECURITY" CONCEPT AS A STRATEGIC FRAMEWORK FOR THE GLOBAL SECURITY-GLOBAL PUBLIC HEALTH INTERFACE

The speaker explored the concept of "human security" as a strategic framework for dealing with global health and security challenges. According to him, we lived in a new threat environment. While faced with new threats like the anthrax incident, old threats like natural disasters and man-made disasters remained. It was also highlighted that when the U.S. Homeland Security Department was created, the definition of the term "homeland security" primarily focused on nefarious threats, for instance, the prevention of terrorist attacks on the United States. However, as a result of Hurricane Katrina, the definition has since expanded to include all threats, hazards and adverse incidents (natural or man-made).

He reminded the audience that whether it was Mother Nature or the mother of all terrorist attacks, there was a need to be equally prepared and equally resilient. He elaborated by sharing that in the summer of 2000, the OEM (Office of Emergency Management) actually initiated the bio-terrorism protocol in New York City in response to the West Nile virus because they thought they were under attack when they started seeing dead crows and other birds in Central Park, New York. This turned out to be an act of nature but they certainly did not know it at that time. He added that as diseases did not recognize international borders, it was essential to take a regional approach. While building capacity at the country level certainly could not be neglected, it was important to work across regions so that individual countries did not become vulnerable to disease transmissions from their neighbors.

A pandemic was much more than just a medical issue. All elements of our critical infrastructure might be affected. Hence multi-sectoral, interdisciplinary approaches were needed. Elaborating on the interconnectivity of the multi-sectoral issues and sectoral interdependencies, he gave the example of the U.S. anthrax letters incident in 2001, and how Washington's PEPCO, the only electrical/power utility company serving the nation's capitol at the time, almost had to shut down its operations following the incident, as they had insufficient cash flow to continue providing power to Washington.

For the speaker, one potential approach to the multi-sectoral challenges of today was to utilize the human security concept that was first promoted by the UNDP in 1994 through the Human Development Report. This concept was attractive because it was people-centric rather than centered on the sovereign state. As it was people-centric, security threats could be gauged through either first-, second- or third-order effects that would ultimately affect the individuals.

He concluded by stating that if one looked at the nature of current challenges to security, there was increasingly tremendous interconnectivity between the various sectors. The recommended way forward in tackling the seven categories of human security threats (economic, food, health, environmental, personal, community and political security) was a human security approach to multi-sectoral resilience.

DISCUSSION

The audience sought clarification on how China's use of trade routes across the Arctic through Russian waters was a potential security problem. A speaker explained that China was used only as an example and was not the only country heading up to the Arctic. It was difficult to navigate through the Arctic waters, and very dangerous from an environmental security perspective. Furthermore, unlike the Suez, the Arctic was unmonitored. There was no verification of the ships, and nobody knew the state of the ship or what was on the ships. All these factors could pose a security threat.

In answer to the question on the analytical and managerial tools needed to be developed to better understand the complex interconnected security challenges, a speaker responded that, as with every community of interest (COI), there was a need to understand each other better, so tools that helped to map or visualize the problem and issues and how they might be interconnected would be very helpful as a starting point.

The audience was interested to know if warning indicators, specialized warning products, and other traditional tools used to rate the level of threat over time were used in individual or integrated communities. A speaker pointed out that no U.S. ambassador had ever declared an event a disaster because of economic or political issues. It was only if an event had a negative health effect on the population that it was declared a disaster. Health became not necessarily a tool but a common measure across sectors, for instance, in the humanitarian arena, rising crude mortality indicated failure. So it was not just about developing new tools. In some cases it was more important to define more sensitive tools from a societal perspective.

ILLICIT TRAFFICKING COI:

EMERGING CHALLENGES IN ILLICIT TRAFFICKING

The panel focused on emerging trends and strategies to address illicit trafficking. Three evolving conditions influencing illicit businesses identified were globalization and technological advances, the ability to influence or control civil governance and legitimate commerce, and opportunities to leverage aspects of human geography. The speakers also discussed the limitations of current border risk management strategies and assessed the management of non-traditional threats in Asia that prioritized the security of the state's sovereignty over those of the individual and society. A tool to address these issues presented was the use of concept maps depicting key genres of international illicit trafficking and money laundering.

MAPPING ILLICIT TRAFFICKING – THE JOURNEY AND THE HORIZON

The speaker gave an overview of the concept maps of illicit trafficking and its future direction. He began by highlighting the link between serious organized crime and the issue of societal resilience. The Home Office estimated that serious organized crime had so far cost the U.K. public over £20 billion in terms of social harm. Although transnational organized crime was often seen to operate in isolation from mainstream society, in reality it was present in every facet of, and affected, the daily lives of citizens. As such, in terms of building resilience, the potential of serious organized crime to destabilize states was something that should not be overlooked.

According to the speaker, the idea of formulating concept maps began in 2007 as a new way of looking at and understanding the issues concerning illicit trafficking. The maps were developed in three parallel sections, involving the testing of case histories to determine its strengths and weakness, the expansion of the map through the addition of new layers of commodities and trafficking activities, and the development of the map with other tools as a mechanism for effective intervention against trafficking organizations.

Regarding the characteristics of the maps, it was explained that they were designed as qualitative models covering the logic behind illicit trafficking from the criminal entrepreneur's point of view. In putting together the maps, four steps were involved: the development of the core "engine" driving the system; the expansion of the maps through the inclusion of environmental variables; the segmentation of the map into relevant commodities and areas; and the embedding of the maps in a futures scenario framework.

He proceeded to elaborate on four possible uses of the concept maps: a heuristic tool to explore and support hypotheses for data gathering and theory building; a knowledge management tool to organize available knowledge; a diagnostic tool to effectively consider investigations by, for example, contrasting what was known in terms of intelligence and what was depicted in the maps; and an operational tool to identify leverage points. He noted that the maps were not predictive tools to anticipate the behavior and activities of launderers. They could, however, be used to test against a range of futures scenarios.

In conclusion, he reiterated that while globalization had brought along with it many benefits, it had also provided opportunities for and become the main facilitator of organized crime. Globalization had in effect increased the pace of all crimes and provided an environment for new crimes to be committed.

ILLICIT NETWORKS IN AN AGE OF GLOBALIZATION

The speaker presented on the introduction of a new project on illicit networks in the age of globalization that would be examined in an upcoming workshop in February 2011. While the growing interconnectedness from reduced barriers to the free flow of information, goods, capital, services, people and ideas might be the major driver in shaping the world, it had also created opportunities for illicit trafficking networks. Some of the key questions and issues that the workshop would examine included how illicit criminal trafficking networks were evolving in response to globalization trends, the ability to develop and exploit new technologies to further the illicit trafficking business, the development of new opportunities for illicit traffickers to influence civil governance and legitimate commerce, and the effects of changing patterns of migration, urbanization and growing resource scarcity on illicit trafficking networks. The workshop aimed to build on the existing work done on the illicit trafficking concept maps. While the maps covered the business infrastructures underlying illicit trafficking networks and how they were embedded in the external environment, the workshop would also consider changes affecting the external environment and its impact on the networks in the future.

Expanding on the details of some of the themes that the workshop proposed to cover, she noted that while new forms of technology, communication and transportation

drove global interconnectedness, it also fuelled the increasing complexity, sophistication and speed of illicit trafficking, allowing age-old criminal activities to take place across vast distances. This meant that there were now worldwide implications in situations where governments were unable to keep in control illicit trafficking activities within their borders. Further, criminal networks had long used bribery, extortion and intimidation to influence public officials in order for them to conduct their illegal business in areas with limited oversight. The workshop aimed to explore how globalization might further enable illicit trafficking networks to challenge the legitimacy of civil governance and exploit weaknesses in governments.

The interaction between criminal networks and legitimate commerce was another area to be explored at the workshop. Criminal networks had often taken advantage of existing formal financial systems, for example, disguising their illicit transactions amid high volumes of legitimate transactions, using containerized shipping to smuggle illicit commodities or bulk cash, using the informal value transfer systems known variously as "hawala", "hundi" or "flying money" and navigating the world of virtual money. These systems created opportunities for traffickers and the workshop aimed to understand how they stood to benefit from the growing global, financial and trade linkages as well as the scale that such criminal networks might be able to influence legitimate commerce.

The final theme that the workshop proposed to explore concerned a few main components. First, increased population growth and economic development would drive increasing demand for scarce resources. This would present new or more lucrative opportunities for traffickers of a variety of commodities, including rare hardwoods, endangered species and precious minerals. Second, migration was likely to increase in the coming decades as people sought new economic opportunities or better security. This was likely to create new and enlarged diasporas, which would also increase the freedom of movement and recruitment opportunities for trafficking networks. Finally, growing urbanization might create a more hospitable environment for traffickers. Already, more than 50 per cent of today's populations lived in cities. This was expected to increase to about 60 per cent by 2030. In some cases, governments could not provide basic services and security to their citizens, allowing criminal networks to step in and fill the gap. This could in turn lead to situations where parts of cities would become essentially ungoverned places but with global connectivity to the rest of the world. The impact of such impending situations would be explored in more detail at the workshop.

THE FUTURE OF BORDER RISK MANAGEMENT – A CRITICAL LOOK AT SOME KEY PROBLEMS WITH BORDER RISK MANAGEMENT AND SOME CONSIDERATIONS FOR THE FUTURE

The speaker began his presentation with two general observations regarding border risks. He noted that, first, the range of issues dealt with at borders are numerous and complex and, second, there are issues with how effective current border control measures were, given the fact that its impact had not been consistently felt. An example of this was the supply of cocaine. While the amount of cocaine seized had increased over the past 30 years, this had had no effect on its street price, which had been decreasing while the quality had been improving.

The speaker was of the opinion that the solution to the above issues was in the implementation of proper risk management measures that would enable the focus to be on what really mattered in a situation where resources were limited. He noted that there were two critical components of risk management: risk assessment and risk mitigation. Risk assessment was defined as the systematic determination of priorities by evaluating and comparing the level of risk against predetermined standards, target levels or other criteria. He noted that the methodology of assessing risk currently in used in Canada, which relied heavily on seizure reports, needed to be revised, as this led to disproportionate risk ratings and the use of resources, especially in cases where there were few reported seizures of harmful substances.

Touching on the elements of a draft risk-assessment model he had been working on, the speaker explained that border risk would be viewed as the equation of the likelihood of non-compliance times the impact of the event. The impact of the event was defined using the variables of vulnerability, scope, consequence and outrage. However, he pointed to the fact that there would be difficulty in measuring the impact of such an event and that a robust methodology was needed to do so. The second critical component, risk mitigation, covered the nature of the problem and tailored solutions to specific risks. He noted that in many instances, big problems could be solved using innovative, precise and targeted methods.

He concluded by reiterating that border control was not going to get any simpler and the future of border risk management lay in understanding the impact of the different issues and establishing a hierarchy of risks in order to concentrate on what was important.

HUMAN TRAFFICKING IN ASIA: TRENDS, ISSUES AND CHALLENGES

The speaker presented on non-traditional security threats, specifically on the threat of human trafficking. She noted that non-traditional security threats were essentially a framework used to examine a slew of security challenges, including illicit crimes, health security and food security. This framework examined the main question of how these issues impacted not only the security and the resilience of states but, more importantly, also on individuals, communities and societies. In this context, the focus was on building resilience of the communities directly affected by such challenges.

It was pointed out that human trafficking affected 12.5 million people worldwide. Asia, in particular Southeast Asia, was considered one of the major destinations of human trafficking, with victims detected in more than 20 countries. Crimes in human trafficking were committed mainly for purposes of sexual exploitation and forced labor. Other purposes for human trafficking included the removal of organs and body parts, illicit begging, forced marriages, illicit adoption and exploitation in armed conflict. Most frameworks available in dealing with these issues involved looking at the challenges in terms of the human security issues of protection. However, the speaker put forth the argument that states needed to work with other sectors, especially civil society organizations and the media, to combat such crimes.

The speaker noted that the media was instrumental in helping to illuminate the nature of the problem. In many cases, human trafficking was not just an issue of criminality. When it was seen from the perspective of the victim, it involved elements of human deprivation such as poverty. However, there were challenges as the media in some countries faced constraints when publishing news on human trafficking issues, which were considered sensitive topics while some media were given to sensationalizing their reporting in order to increase sales. Civil-society organizations were important actors in helping to prevent trafficking and in intercepting and rescuing victims. They also played a key role in reintegration programs, helping victims find work opportunities as well as deal with psychological issues.

The speaker concluded by stressing that while there had been progress in the way human trafficking issues had been addressed in Asia, there was a need for more engagement from actors other than state agencies. While human trafficking was essentially treated as a criminal act, more effort was needed to examine the protection of its victims. This underlying tension of trying to address a transnational crime and the need to focus on what were essentially issues of human rights remained one of the major current challenges. A way forward might be to examine how government agencies could work to build more linkages and partnerships with different actors with a stake and a role to play in human security.

DISCUSSION

A participant raised the question of whether it was feasible to reintegrate victims of human trafficking, as there were instances of them being killed or ostracized, and further, whether there was existing research on effective ways to introduce safe places for such victims to live. A speaker stressed the need to differentiate victims who were trafficked victims with those who have left their countries for fear of being persecuted there. She cited research done on the experiences of Cambodian trafficked victims, noting that attempts at reintegration failed primarily because of the deficiencies of the program designed for the victims. There was a need for a comprehensive system of support for victims encompassing things like assistance to secure employment and getting through the psychological and emotion trauma suffered.

A question was raised as to whether there were examples of how the concept maps for illicit trafficking were used as an operational tool or in an actual operational situation. A speaker recounted a particular case where the concept maps were used to analyze a huge amount of data obtained in an investigation. He noted that it was an effective method of exploring data that led to the realization that a broader focus was needed for a more effective investigation.

A question was posed to the panel as to whether there was now a paradigm change in terms of countries of destination and origin in the context of human trafficking and, if so, which countries played a greater role. A speaker noted that in terms of looking at it from the perspective of the victims and considering some of the frameworks that were emerging in Southeast Asia, there was a changing paradigm in the region and the reason for this was the presence of different communities advocating for change, involving not only the criminalizing of human trafficking but also protection issues. Another speaker brought up the fact that climate change in the future was set to have a massive effect on migration patterns, creating a class of climate migrants.

Another question raised concerned whether the perspective of criminals was used in the creation of the concept maps. A speaker replied that it was part of the challenge the team had faced when they needed to put themselves in the shoes of the criminals without involving any criminals. In approaching this challenge, the team enlisted the assistance of not just experts from law enforcement but also, among others, those from the United Nations, financial regulators, persons from treasury departments and money laundering investigators.

EMERGING AND DISRUPTIVE TECHNOLOGY COI: REPORT ON CYBER SECURITY AND DISRUPTIVE TECHNOLOGY

The panel addressed challenges to cyber security and energy security. Obstacles to mitigating threats to cyber security include the lack of cooperation among government agencies and the dearth of expertise on emerging technological complications. The presentations also covered the limitations of cloud computer security and an overview of the Italian government's approach to cyber security. Given the transnational nature of the problem, it was stressed that international collaboration to tackle the problem is critical. The presentations on energy security covered the challenges arising from increasing global energy demand such as energy sustainability and carbon dioxide emissions. The need for substantial investment into research and development work on clean and efficient energy technology, and policies to curb any further carbon dioxide emissions was stressed. The prospect of energy conversion technologies and how changes in current energy consumption choices could be beneficial to long-term environmental conservation efforts were also discussed.

THE LARGER SECURITY CONTEXT OF CYBERSPACE

The speaker explored the larger security context of cyber developments. In particular, he spoke on the range of interlocking security problems that arose as a result of the pace and scale at which system integration was taking place in the cyber sphere.

In his opinion, cyberspace encompassed more than just the Internet and included technologies and systems that smart phones and power grids, for instance, functioned on. Similar to the impact that technological advances in the transport sector had on societies and cultures during the earlier stages of globalization, it was noted that cyber developments had also brought about a massive rapid transfer of goods, people and information over large-scale networks. As such, disruptions to any nodes would have cascading effects on critical infrastructures that were dependent on the web for its daily functions and operations. He added that given the high level of connectedness between global and local critical entities, and the ease of accessing web-based facilities these days, it would be difficult to predict or pre-empt a cyber attack quickly. This inevitably complicates policy decisions since we would be moving into unchartered territories where critical infrastructures were web-based.

Advances in networking tools and applications (for example, Web 2.0) have also changed the way people communicated and engaged with one another. The speaker opined that we were moving into a world where everyone was capable of gathering data and projecting their influence through the web. In a cloud-computing environment, for instance, information could be distributed seamlessly over complex networks. As such, we would have to confront a whole new spectrum of malicious acts conducted by actors ranging from hackers to terrorist groups.

A key challenge in cyber security was the development of new theoretical frameworks that could support sense making and foresight. On the one hand, advances in cyber technology had facilitated data collection and improved computational capabilities. On the other hand, it had made the harvesting of information for criminal and illicit purposes easy and also created a problem of privacy. The cellular phone, for instance, could be tapped for crucial personal information. Moreover, the way the Internet was organized had made it very easy for anyone to cover their tracks and create mayhem. On the whole, cyber security called for the cooperation of various government agencies and the private sector. It was a problem that was generally not addressed fast enough due to existing stovepipes and the lack of expertise to deal with emerging technological complications. It was also a global problem that required international collaboration, as it implicated jurisdictions and cut across societies.

In view of the borderless nature of cyber-related issues, it was suggested that a similar structure like the Intergovernmental Panel on Climate Change (IPCC) be considered for cyber security as well. It was thus mentioned in conclusion that the GFF, with its international and diverse membership, fit the bill. In fact, it could well be the platform for the tackling of cyber threats from an international policy level.

CLOUD COMPUTER SECURITY – THE SOFT SPOT

The speaker explored in his presentation the pitfalls of cloud computing and how online applications might be manipulated for criminal activities. Cloud computing had been marketed as a cost-effective and innovative IT resource-sharing and management platform. However, he warned that in the pursuit of cheap and fast IT solutions, applications were often developed without security as their top concern. It seemed that most individuals and organizations either assumed that conventional security measures were sufficient to deal with new cyber threats or prized other operational requirements over security. For example, it was stressed that in the current work environment, crucial computer security elements such as confidentiality and integrity were often overlooked

in the pursuit of information "availability" and being interconnected. In his opinion, the basic blocks of computing security should not change even with the subscription to cloud computing.

The range of security tools used to protect systems and networks these days were not adequate. In the past two decades, firewalls, antivirus and vulnerability scanners, for instance, had been the only ways to protect cyber infrastructures against attacks. However, they were no longer adequate and gave a false sense of security. Modern hackers were highly capable of circumventing firewalls and disrupting business functions through application attacks. As an illustration of the ability of hackers to gatecrash firewalls, the speaker mentioned that the Federal Aviation Authority's website was recently hacked. While no key data or plans were stolen and crashed, it demonstrated the limitations of our existing cyber-security tools and solutions. The basic premise was that hackers were well-versed in the range of cyber-security tools currently in use and had found new ways to compromise data through software and application attacks.

Until recently, software and application attacks were not thought to be common. Current communal security infrastructures such as firewalls and encryptions were thus built to protect mainly systems and networks. Hackers were quick to tap on this security gap and launched their attacks via applications and software. This problem was further compounded in that system and network administrators were usually not well-versed with application developments. Likewise, application developers were usually more concerned with writing their applications according to their client's requirements than with incorporating security features. Applications could therefore be easily tapped, manipulated and crashed by hackers to reveal crucial personal and corporate data. The speaker shared, for instance, that error and debug tool messages readily broadcasted to hackers the IP addresses of key architectures (for example, server and client information database). This could have been avoided had applications been written "properly" to limit such information for "internal consumption" only and not disclosed freely over public cyber domains (for example, search engine results and debug messages). While, admittedly, it would be difficult to screen and check every application for security loopholes, he asserted that had security been part of an application's initial design, online application crashes and information thefts could have been minimized.

In conclusion, the need to incorporate security into software and write applications with security in mind was underscored. The speaker also reiterated that current communal security infrastructures were not built to protect software and applications. It could not be assumed that firewalls or even applications on their own could ward off all forms of cyber attacks, especially, those on shared software in a cloud-computing environment.

GLOBAL ENERGY FUTURE AND ENERGY SECURITY CHALLENGES

The speaker explored the security implications of current and future energy consumption. As the world's current largest energy source, liquid fuel was projected to continue to be the main fuel source for the world's transportation sector. However, renewable, nuclear and coal energy consumption was projected to increase most significantly in the next two decades. The International Energy Agency had also forecasted that energy consumption by non-OECD (Organization for Economic Co-Operation and Development) countries—particularly China—would rise the most in the same period. It was also projected that the world would increasingly turn to nuclear energy sources in the next 20 years. These energy projections were based on current energy consumption levels and industrial activities worldwide.

The speaker noted that energy use was unlikely to fall in the coming years. In fact, it was projected that world energy demand would increase by approximately 50 per cent between 2007 and 2035. It was also added that the energy demand increase would almost exclusively be driven by non-OECD countries' growth. This would inevitably raise questions of energy sustainability, carbon dioxide emission and energy security.

The definition of energy security differed according to the energy needs of each country. What was essential, however, was an understanding that energy-related issues and challenges were often interrelated and had implications on other security concerns. The energy needs of all countries must be reconciled before there could be any consensus on global energy security matters. Essentially, the four key components to energy security were resiliency, collaboration, diversification, and production, conversion and usage. The speaker explained that resiliency had implications on a country's "security margin" and diversification on supply sources and networks. On the other hand, collaboration from a policy point of view affected the way global interest and cooperation on energy security was consolidated and promoted. The last component concerned the way technologies were harnessed for the production, conversion and usage of clean energy sources.

In conclusion, he emphasized that increasing global energy demand in the near and long term would give rise to additional energy security challenges especially in areas concerning energy sustainability and carbon dioxide emissions. In particular, he highlighted the need for substantial investment into research and development work on clean and efficient energy technology. This should also be supplemented with policies that curb any further carbon dioxide emissions.

ENERGY SECURITY AND POTENTIAL GAME CHANGER TECHNOLOGIES

The speaker presented on the prospect of energy conversion technologies and how changes in current energy consumption choices could be beneficial to long-term environmental conservation efforts.

In his opinion, oil as an energy source would never run out. As a matter of fact, oil only formed about 26 per cent of the global energy consumption mix. Rather, what should be of greater concern was how to transit to a more energy-sustainable future. This would entail investments into the development, deployment and usage of low-cost but environmental friendly energy conversion technologies. At present the key challenge was the deployment of renewable or conservable energy sources on a large scale. The knowledge to convert energy existed but large-scale deployment was still too costly for many economies.

The technology and skill to convert coal into liquid fuel, for example, had long existed but it was still not yet an environmentally friendly process. Shell, as an International Oil Company (IOC), announced plans to invest more in sustainable energy sources like natural gas by 2012. This would be followed by many other IOCs in the near future. However, the speaker maintained that this transition was not driven by an oil shortage but triggered by technological advances that allowed for the renewal and sustainable

consumption of energy. This, in his opinion, underlined the concept of disruptive innovation in that it was not just the technologies but also the management and deployment processes that affected the way we developed and consumed energy altogether.

In general, it took three generations for any new energy technology to mature to a stage where it was time and cost efficient to produce on a large scale. This process of refinery often prevented countries from adopting more sustainable energy options. It was noted from personal experience, for example, that utility companies might not be keen to offer renewable energy technologies to their consumers, as it would affect their revenue. This therefore led to questions on the potential gains in energy technology changes. It was noted that, of the available energy sources to date, coal and uranium were going to be the primary sources of energy to keep a close watch on. The former would most likely make a comeback as a major energy source, as China developed and drove global demand for it. Technologies to harness uranium for energy were improving and in the not-too-distant future, the ability to tap into uranium for terra-energy would prove to be a tremendous gain for countries. However, it might be at the expense of environmental degradation as clean coal technologies and solutions for the proper disposal of nuclear waste were still not readily available.

The focus in the short and medium term was therefore how we might use a spectrum of energy sources and conversion technologies efficiently without placing further constraints on the environment. The speaker concluded that it would probably be a challenge to convince economies to adopt existing or new energy conversion technologies when the incentives were not there. However, the fight was not all lost, as increasingly we were seeing countries like India and China investing into efficient energy technology like smart electricity grids and this marked a transition from being consumers of renewable energy to producers.

LUNCH KEYNOTE

The lunch keynote explored the growing part that intelligence had been playing in supporting modern national security strategy and, in turn, the importance of building up resilience as part of the national security strategy. A key argument was that national security policymakers would need strategic notice of possible threats and hazards if they were to invest wisely in resilience but it was important to note that this function differed in many ways from the traditional intelligence assessment, which was more focused on forecasting than prediction.

IS RESILIENCE AN INTELLIGENCE ISSUE?

The speaker began by highlighting three important ideas. First, the ability of a nation to keep going under sustained disruption depended directly on how resilient the

infrastructure systems such as power were, as well as how vulnerable things like the logistic lines of communication were. Second, by trying to disrupt the infrastructure that supported everyday life, an adversary could indirectly try to affect the psychology of the public, causing serious dislocation to the home front and thus influencing the political will of the nation to keep going. Third, the national authorities in those circumstances could certainly organize themselves to do their best to recover from whatever had happened, working, for example, with private industries to minimize disruption. However, the most important lesson was not to have major vulnerabilities that could be disrupted in the first place.

Those three lessons could be linked directly to what the speaker described as the three generations of resilience thinking that have taken place in the United Kingdom,

spurred on particularly by 9/11. He described first-generation resilience thinking as an outgrowth of Cold War planning that aimed to protect key points and nodes should war or, in the present context, terrorist attacks occur. Such an approach had great value but was limited because it was difficult to identify where the points of failure were in a complex set of systems. Second-generation resilience thinking was designed to reduce risks at a more fundamental level, by improving the resilience of the local community itself, including psychological resilience. He provided the example of setting a community level local resilience forum, where the local government emergency services industry, voluntary sector and community groups could meet to work out how to help each other should a disruption occur. This led to what the speaker believed governments were embarking on now, a third generation of resilience thinking—adaptive resilience—in which the lessons of past crises were applied to the design of regulatory frameworks and new facilities. Secured by design, for example, was a set of standards for the engineering and building industry in the United Kingdom that would ensure all new buildings and facilities were designed with security in mind.

The speaker put forth three propositions to help secure the state. The first was to see national security in terms of a state of normality. The public, markets, allies and even adversaries needed to derive from a sense of confidence that societies were capable of managing risks successfully. The second was a recognition that the sense of security rested on the sensible management of risk and not on its elimination, for example, by pre-empting disruptive challenges wherever possible, investing and advancing in the reduction of vulnerability, preparing oneself for events when they happen. Third, he identified the key to foreseeing problems before they occurred and maintain the delicate balance between the needs of security and the needs of civic harmony and upholding justice and the rule of law, to be better informed at decision making by government, which was what intelligence existed for.

The speaker noted that intelligence could help the decision maker at three levels: by providing situational awareness—the who, what and where; by providing explanations—the why and what form; and by prediction—what next. However, decent predictions are only possible if it is based on sound rationale. The intelligence community had been accused of not joining the dots, but the real key was whether there was strategic notice of the hypothesis. The best strategic notice tended to come out of the scientific community. With strategic notice, one would have the ability to cue one's intelligence service so that they would know when a pattern of dots actually represents a warning signal that might then lead to operational alerts.

The speaker concluded by stating that the intelligence community needed to understand the modern concept of resilience and its three generations. They should not just be able to support military planners in conventional operations but to also get inside the minds of non-state actors and terrorist groups to understand how they think. The intelligence analyst also needs to understand how thinking within the intelligence community was developing, as we know more about infrastructure in the current cyber age. Only then could the intelligence community support the resilience planners.

DISCUSSION

How statesmen create resilience in a population that had lost its belief and vision in the old-fashioned grand narratives was discussed. Leadership, according to the speaker, was the answer. He believed that Lee Kuan Yew was a good example of high-level leadership. The influence Lee had at the very beginning on how the state of Singapore should develop—by having a very simple set of principles that would then infuse all thinking in policy making, including being part of a global trading community—was the basis for social resilience in Singapore.

The audience wanted to know how societal resilience could be measured. The speaker replied that there were plenty of indicators that could be set up, such as feedback from people engaged in activities specifically designed for enhancing resilience and polling public sentiments to gauge whether people felt confident that things would be managed. Furthermore, when faced with the odd resilience challenge, it would quickly become clear if your systems worked.

It was debated whether resilience planning was best not talked about lest it be seen as a challenge that maligned groups might take on or invited local resentment and accusations when the government responded inappropriately. To this, the speaker answered that governments should never use phrases like "we will ensure it will never happen again", as it would give people a false sense of security. Put differently, over-promising and under-delivering should be avoided. However, he believed that it was possible to build a strong sense of commitment to resilience through cultivating local pride. He felt that there was actually some deterrent effect in showing that the nation was actually not going to be driven off course by attacks. After all, if the terrorists' objective was to disturb normality and the government's objective to maintain it, demonstrating that a nation had what it takes to be resilient could be quite a powerful force.

STRATEGIC FORESIGHT AND WARNING COI

The panel explored the enhancement of global and national security through strategic foresight and warning by addressing issues of methodologies, best practices, organizations and alternative ideas. The presentations focused on the British and U.S. experiences in producing actionable foresight. It was noted that the development of strategy required the practice of questioning assumptions and being upfront about uncertainty, the engagement of policy-makers, efforts to highlight not just threats and problems but also opportunities, and an understanding of the vision that policymakers were seeking to achieve. It was also suggested that the intelligence maintained close relationships with think tanks and academics in order to be exposed to new ideas from different sources.

CAN FORESIGHT BE ACTIONABLE TODAY?

The first speaker elaborated on the background of the Strategic Foresight and Warning community of interest (COI). She explained that this COI was set up for the purpose of contributing to the enhancement of global and national security by promoting the best possible strategic foresight and warning.

The COI aimed to promote exchanges between those who participated in strategic foresight and warning across communities of analysts, strategists, planners, policymakers, researchers and those in the private sector. These collaborations would work towards identifying and reflecting on effective and ineffective strategies, common challenges and potential solutions. The COI addressed a vast array of topics, such as issues of methodologies, best practices, organizations and alternative ideas through networking, projects, conferences, workshops and participation through websites.

She concluded by inviting participants to raise and suggest topics that they were interested in and could potentially be explored by the COI.

The second speaker presented on the British experience in making foresight actionable. He began by assessing foresight work in three different kinds of activity: whether there had been an improvement in the use of foresight in looking strategically at individual government policies, whether there had been an improvement in building strategies at a national level in terms of dealing with issues such as countering terrorism, nuclear power and reducing juvenile crime on which the resources of the state had been invested in securing, and whether it was possible to use foresight to construct grand strategies by setting out principles that the nation should be governed by.

In considering the three categories, at the first level, there had been a proliferation of strategy units and the problem with this was that there were too many strategies that did not add up to a cohesive national strategy. Secondly, with regard to producing government-wide functional strategies, it was noted that it was easier to publish a strategy than to implement it. A counter example to this was the U.K. counterterrorism strategy, which was drawn up in 2002/2003. It was still in place after eight years because it had strategic logic built into it in terms of risk management. It was explained that while the third level, which involved the construction of grand strategies, was not something that had been attempted during recent times, this seemed to be something that the new government in place was attempting. This illustrated an important point about attaining actionable foresight, which was the importance of political leaders in the process of building the strategy. He stressed that in the past, a lot of good strategic planning did not engage the political leadership, making it harder for the leadership to accept the plans.

One of the key inputs needed was strategic notice, which was closely connected to horizon scanning and foresight work. The speaker explained the difference between foresight and prediction, stating that the goal of the intelligence community was to predict whereas foresight presented a range of possibilities to policymakers. Those involved in both foresight and predictive intelligence work needed to remember that they were engaged in what the ancient Greeks described as phronesis, defined as "the application of good judgment to human conduct consisting in a sound, practical instinct, an almost indefinable hunch, which anticipates the future by remembering the past and thus judges the present correctly". He stressed that decision makers were human and were subjected to cognitive biasness like every other person, but had the additional problem of being under media scrutiny, which made every single thing they said and did liable to becoming a matter of political controversy. This was one of the main challenges in obtaining foresight that was actionable.

In conclusion, the speaker reiterated that the development of strategy required conceptual thinking. It would take very good and well-presented foresight to persuade governments that sacrifices had to be made now for the benefit of the future.

The third speaker addressed the issue of actionable foresight from the perspective of the U.S. analytic community. First, he stated that there was no substitute for broad and deep subject-matter expertise and for compiling the best analytical work from both inside and outside government.

There was also the responsibility to reach out and liaise with the best experts around the world to deal with the relevant issues before them.

His second point involved the constant focus of the foresight community on threats and problems. He noted that while this was understandable, it was not necessarily helpful for the policymaker. As such, where possible, efforts should be made to highlight opportunities to policymakers as well.

On the third point, it was stated that there was a need to be upfront about uncertainties. In their line of work, the foresight community had been involved in studying the drivers of behavior, key things that would shape countries, spell out alternative scenarios and present to policymakers their judgment about where things were going. As such, the practice of questioning assumptions and being upfront about uncertainty was important.

Lastly, the speaker stressed the need for engagement with policymakers. He noted that the work done would not be actionable unless there was continuous dialogue with policy customers, including the planners who could give feedback on when the information was helpful and when it was not. A balance also had to be struck between being prescriptive and providing information advantage that policymakers needed.

The fourth speaker spoke on the issue of actionable foresight from the perspective of policymakers and presented three observations. First, she reiterated the importance of the need for foresight analysts to continue with their work as what was produced was used and considered by policymakers. In connection to this, she explained that policymakers were sometimes not able to comprehend the workings of foresight analysis and, as such, a better understanding of methodologies and context would help make such analysis more usable. She explained that one of the reasons why Global Trends 2025: A Transformed World, published by the National Intelligence Council, was so important. It contained not only a U.S. perspective but encompassed global views as well. There was therefore the need especially for those in the foresight community to be more collaborative and sensitive to global trends.

Second, moving to the actionable, the speaker noted that it was important to understand the vision that policymakers were seeking to achieve and to reflect this in foresight analysis. This would provide the framework for the foresight community to engage in dialogue with policymakers. Further, challenges being faced today had to be resolved together and not individually. As such, there was a need for the foresight community to propose solutions that were more collaborative in nature.

Finally, the speaker called on the foresight community to remain optimistic that the work they were involved in made

a difference. She concluded by reminding the community of the importance of maintaining close relationships with think tanks and academics in order to remain relevant and be exposed to new ideas from different sources.

DISCUSSION

A participant spoke about the necessity to add multi-disciplinary content to any strategic foresight work, adding that while traditional military and political issues were usually considered in foresight analysis, in the long term other issues such as those dealing with non-traditional security matters might turn out to be challenges that would be more overwhelming. A speaker agreed that it was important to look beyond the traditional national security communities, adding that the experience in the United Kingdom had been that the broader scientific community had proved to be further ahead in providing usable foresight, partly because it was easier to identify the leading edge from the future path of scientific development. Another speaker added that the best U.S. analytic products had always been those that were multi-disciplinary in nature, involving the most outreach and interchange. Moreover, fermentation and dialogue were invaluable in shaping the work done by the foresight community.

A participant raised a question concerning foresight as an intelligence function and whether one of the ways to make it more actionable was to make it more accessible and to get policymakers more engaged. A speaker noted that the intelligence community was deeply involved in the work, although they did not monopolize it. He opined that the intelligence community could gain from foresight analysis as the information could help them connect the important dots in their work. Another speaker concurred that it was not only the intelligence community that produced foresight and scenario planning; think tanks and private groups were involved in these areas as well.

A participant raised the question of how to take the good work of foresight analysis and best translate it for policymakers in a useful manner. Referring to the presentations on Singapore's experience, she asked whether this method was a good technique in delivering foresight messages to policymakers. A speaker noted that the method used by Singapore would resonate with policymakers and that a lot of information could be communicated in a very short time.

A participant noted that one of the characteristics of foresight was that often times it conceptualized and envisioned multiple alternatives and in that sense the information was often less rich in data, facts or evidence in comparison to actionable intelligence or the data that drove tactical decisions. He queried whether decision makers who were anchored to the belief in the value of evidence-driven decisions were less accepting of the

usability and attractiveness of foresight analysis due to the absence of facts or evidence. A speaker noted that foresight was a process of describing how things might unfold and it was not a description of fact. Policymakers did see value in a product that was quite light in terms of facts as they would have to deal with the same questions themselves when they planned for the future. Governments had to make decisions that would affect the next 5 to 10 years, whether there was intelligence supporting their decisions or not. Another speaker stated that foresight analysis was based on patterns even if the relevant data were not available.

A participant asked the panel to address the issue of whether it was worthwhile to prioritize and aggregate security challenges and, if so, how this was done. A speaker stated that in his experience, policymakers were usually asked what their priorities were and the analysis of foresight analysts responded directly to that list. Where there were issues that were thought to be emerging and needed attention, this would be brought to the policymakers for their consideration. Another speaker noted that if a list of security challenges was drawn up for the United Kingdom, the risk of an attack by a hostile power would be ranked low due in part to the presence of NATO. Referring to this example, he stated that placing risks on a list could be misleading unless the dynamics involved were taken into account.

LOOKING AHEAD TO A GFF RESEARCH PROGRAM:
CROSS-CUTTING ISSUES

This panel offered a look into some of the issues which cut across communities of interest within the GFF. Here speakers highlighted some of the areas in which future collaboration and further research was required in an ever changing political landscape.

BRIDGING THE GAPS AND THE NEED FOR FUSION

The speaker argued that the change in the nature of security threats since the Cold War requires a paradigm shift in the mindset of intelligence agencies from "need to know" to "need to share". He highlighted four points of divergence between the role of intelligence and law enforcement officers that hampers attempts to deal with terrorist threats. First, the purpose of intelligence is for policy formulation while the purpose of law enforcement is operational. Second, intelligence agencies gather information that helps in the prevention of an incident while law enforcement agencies focus on responding to an incident. Third, the standards of what constitutes good intelligence for intelligence agencies are not fixed but relative whereas law enforcement agencies require information that stands to scrutiny in the court of law. Fourth, intelligence agencies tend to protect their sources while law enforcement agencies have to make certain sources public for conviction purposes.

He went on to highlight the change in the nature of security threats since the Cold War. During the Cold War, the sources of security threat were namely posed by external belligerent states that were geographically bounded and identifiable. The consumers of intelligence then were primarily limited to political and military officials at the federal level. However, in the current "era of terror", security threats originate not just from state actors but also nebulous transnational non-state actors. As such, the consumers of intelligence have expanded to include state, local and private sectors.

Following from this, the speaker identified five opportunities for further interdisciplinary research. The first is to bridge the military-civilian divide in approaching the terrorist threat. The second divide to be bridged is that between academics and practitioners. The third is to reconcile a top-down approach that most policymakers are used to with a bottom-up approach that engages the practitioners on the ground. The fourth is to break the silos within the intelligence community. The fifth is to enhance the interaction between security and planning agencies within governments.

GLOBAL CITIZEN TRENDS – IMPLICATIONS FOR POLICY MAKERS

The speaker identified global citizens as a potential research topic for the GFF. Noting that much of the debates within the GFF on the engagement of citizens have focused on domestic citizens, he pointed out that the potential for nations to strategically tap on their overseas citizens has not been systematically explored even though the numbers of such global citizens are increasing.

The speaker identified the following issues for further attention. First, the notion of citizenship is evolving and being challenged with greater mobility of populations globally. Second, the actions of non-state actors have

an increasing impact on international affairs. Third, the growing number of overseas citizens is exposed to a broad range of risks abroad. As a result, global citizens pose policy challenges to their governments. For instance, an increase in the number of global citizens impacts government planning, operational capacity and legislation. Moreover, there is growing expectations among the citizenry of what their governments should deliver to them.

Nevertheless, global citizens also present their government with opportunities. First, global citizens could be strategic assets. For instance, they could be valuable partners in responding to crises through web-based platforms. Their international experience could also provide valuable feedback to their government agencies of responses to their policies to address new challenges abroad.

In conclusion, based on the premise of taking a whole-of-country approach to managing risk and resilience, a step forward would be to engage our global citizens more effectively.

CROSS-CUTTING ISSUES IN THE COI POI: PAST AND FUTURE

The speaker provided an overview of the Practice and Organization of Intelligence community of interest (COI POI). The COI POI is concerned with the management, leadership, organization and best practices in the craft of intelligence analysis. Given the sensitive nature of the field, the emphasis of the COI POI thus far has been trust-building and exchanges on non-sensitive areas.

He went on to table four new directions. First, there should be a separate agenda for management and practitioners. Second, there is an interest in approaches to developing young analysts quickly. Third, virtual collaboration through the dynamic use of the GFF website should be enhanced. Fourth, regional COI POI meetings could be held.

DISCUSSION

On the features of a good GFF product or subject area, two speakers were of the opinion that the GFF was unique as it connected intelligence organizations, academics and NGOs from different countries, and adopted a multi-disciplinary approach to develop new insights on transnational issues. Moreover, the GFF should not just bridge substantive topics but also the methodologies and processes both within and across the communities of interests (COIs).

While it was acknowledged that awareness of non-security issues enriched the security sector in government, the panel was asked to identify the value security discourses have for those outside the security sector. A speaker pointed out that in instances where the same issues are being tackled by security and non-security sectors, both sectors could gain by comparing their datasets, assumptions and approaches to the issues to gain new insights for their own work. Another speaker added that while many have called for international cooperation on transnational challenges, few forums exist for this purpose. Hence the GFF has the potential to provide a valuable platform for different countries to come together to develop international rules of engagements to deal with these issues. Noting that the issue of trust building was a work-in-progress, another speaker suggested that breakout groups be added to complement the current GFF format of plenary sessions to allow participants from government to network and discuss sensitive issues with more confidence.

Regarding cross-cutting issues for future GFF research agenda, a speaker identified four key issues for the COI POI: analyzing the relationship between intelligence analysis and diplomacy, adopting multi-disciplinary approaches to the research agendas, dealing with the challenges faced by security sectors owing to bureaucratic upsizing and downsizing, and managing intelligence in federal states. Another speaker suggested developing simulation scenarios for issues of interest.

DINNER KEYNOTE

The dinner keynote discussed the concept of a "relational state" defined as a system of governance that does things with the people as opposed to doing things to or for the people. It was argued that the relational state looks set to become increasingly mainstream, particularly during hard times, when the state will need to justify difficult policy choices and trade-offs. A resilient national response to these challenges may likely require governments to work together in partnerships of trust with their respective societies.

DEVELOPING THE RESILIENT, "RELATIONAL" STATE: FROM GOVERNMENT TO THE PEOPLE TO GOVERNMENT WITH THE PEOPLE

The speaker began his talk by suggesting that the concept of resilience should be thought of in conjunction with two other words that start with the letter R: readiness and relationships. He went on to say that readiness for the

future and the relationships we maintained were essential in overcoming shocks and that we were only beginning to understand resilience in a more holistic way.

He then spoke of his participation in the establishment of the United Kingdom's Strategy Unit. In this effort, the United Kingdom attempted to apply systematic thinking to issues such as education, drug policy, health, energy and fisheries. By linking foresight, scenarios and analysis with the specific design of policies, budgets and legislation, they were able to more effectively developed government strategies. However, he lamented that one of the odd things about the experience was how little literature was available on the subject of government strategy development. The speaker pointed to the enormous amounts of books on military strategy and business strategy but almost nothing was available on the very different circumstances of strategy to deal with the interaction of politics, politicians and the civil services.

The speaker then explained that when working to develop a strategy for government, strategists needed to be very rigorous about two things: power and knowledge. He continued to say that the ability to impact any situation was almost entirely determined by the power at one's disposal coupled with the knowledge that one had to act. Here, he insisted that there were three questions all foresight strategists needed to ask themselves when developing strategy: (i) What do we know? (ii) Where is our power? (iii) If there is a strategy, does it generate the new knowledge we need to capture or maintain power? He cautioned that states were often tempted to believe that they were omniscient and omnipotent, which could be overcome with a healthy dose of humility, skepticism and even doubt.

The speaker then went on to examine the changes taking place in the business sector, where he suggested that businesses were investing heavily in moving towards a relational economy. He suggested that this was something that governments needed to do as well if they were truly interested in developing resilience. The key, he argued, was for governments to look directly at their relationship with their citizens as opposed to setting themselves performance targets. Bringing all these points together,

he argued that resilience was fractal in that a number of issues that had traditionally been examined from the level of the nation state were not very dissimilar from the issues that appeared at the community level of families and individuals. He suggested that resilience, relationships and readiness for the future were similar, whether discussing government or individuals.

The speaker argued that today the question rested upon whether or not we were preparing the next generation with the skills necessary to respond to crises effectively. Specifically, he questioned whether this next generation had in place the relationships necessary, or the collective efficacy needed to act. He described a program that taught resilience to 11-year-olds that he had been running for the last four years. The program had been formally evaluated and the evaluators had found that the students who took part in it not only became more resilient but their relationship with their parents and their ability to think ahead and to set goals for themselves had also improved greatly. He concluded by asking the audience a hypothetical question: If those in the room were given responsibility over the world's seven-year-olds, what would they do with them and how would they prepare them for the future?

DISCUSSION

One member of the audience asked about the relationship between paranoia and resilience, as he felt that paranoia might actually encourage determination and initiative. But at the same time paranoia might be antithetical to resilience in that paranoid individuals acted inappropriately, desperately and over-aggressively. The speaker responded by citing states—such as Israel, Finland, Taiwan and South Korea—that he considered to be somewhat paranoid and quite successful. He went on to say that all states, much like individual human beings, needed to be slightly paranoid in order to survive. However, he cautioned that too much paranoia was not good. If a state were too paranoid it would become incapacitated. The challenge for governments was exactly like that for the individual—a combination of paranoia and a willingness to think creatively and engage would lead to dynamism.

ORGANIZING INTELLIGENCE FOR RESILIENCE

The panel examined comparative national experiences in organizing intelligence for resilience. It was argued that an efficacious risk-assessment process provides a workable set of analytical lenses through which to view national security challenges to prioritize the many competing national security challenges. Some challenges to national security risk assessment include prioritizing national security threats, identifying and comprehending the dynamics and significance of the connections between the increasingly inter-connected security threats, assessing complexity and the lack of consensus over security threats among states. The panel also discussed enhancing societal resilience in the face of crises. This entailed developing trust between the state and people, and also not just an understanding of the resilience of one's own nation but that of the adversaries.

JOINING UP THE DOTS: A METHODOLOGY FOR ASSESSING NATIONAL SECURITY

The speaker argued that a rigorous methodology for assessing national security risk was central to the task of anticipating and managing the proliferation of complex, interconnected "known" security challenges, as well as unexpected "black swan" events. Without an efficacious risk-assessment process, intelligence practitioners would struggle to develop a workable set of analytical lenses through which to view national security challenges while policymakers would not be able to prioritize the many national security challenges competing for their time and attention.

Four challenges to national security risk assessment were identified. The first was how to prioritize national security threats, given the sheer diversity and number of threats confronting nations today compared to the stark parsimonious strategic and intelligence agenda of the Cold War. Second, because many of today's security challenges were highly interconnected, it was imperative to find a way of identifying and comprehending the dynamics and significance of these connections. A third problem was the difficulty of assessing complexity, including positive and negative feedback processes that would amplify or dampen the effects of certain changes. Fourth, due to cultural, historical and strategic reasons, not all states shared the same threat perceptions. Even where there was broad consensus or a common security agenda, there might be significantly dissimilar views about the seriousness or probability of particular risks that no methodology—no matter how rigorous—could resolve entirely because human judgments were required.

Following from this, it was argued that a national security risk methodology for the twenty-first century would constitute four distinct but integrated sequential steps. The first step was to identify—as comprehensively as possible—those issues most likely to have a major national security impact and to aggregate them in a coherent, systematic manner. The second step was to appraise their probability and likely consequences, and to agree on which challenges require further analysis. The third step was capability assessment, of which the principal purpose was to ascertain the country's readiness to address specific vulnerabilities. Rather than attempting to eliminate specific risks, capability assessment should specify ways of enhancing overall resilience so that a country could absorb disturbances and continue to function effectively, even under extremely adverse conditions. Integral to this process was the determination of national security vulnerabilities, which were not the same as threats. The fourth step was to develop a portfolio of national security priorities that treated them as an interrelated whole and provided the basis for a resource-investment plan in national security that was explicitly tied to budget realities.

The speaker then suggested a systems-of-systems (SOS) approach that would address the most serious security challenges as a whole rather than treating them as independent, compartmentalized issues. The SOS approach incorporated metrics that correlated consequences and probability of system-changing threats to determine risk, was based on the principle of sub-optimization and was designed for hyper-complexity.

The speaker concluded that the ability of nation states to develop effective analytical tools for assessing national security risk would be a key determinant of success and failure in a world where the number of security challenges was expanding at such a rate that they threatened to overwhelm the capacity of governments to comprehend their import, develop effective policies and design operational responses. Nations adept at anticipating developments, discerning trends and evaluating risk among the clutter of confusing and contradictory change indicators would be significantly advantaged over those that were not.

ORGANIZING INTELLIGENCE FOR RESILIENCE: AN ISRAELI PERSPECTIVE

The speaker provided an Israeli perspective on organizing intelligence for resilience. He argued that the Israeli discourse on resilience was centered primarily on national security and responses to terrorist threats. Noting that the civilian population had been specifically targeted by their adversaries over the last two decades, there was a growing realization that while the military and security apparatus had a major role in actively suppressing terror attacks, the resilience of the civilian system—their capacity to bounce back rapidly from a crisis—determined the outcome of the conflict.

He proceeded to elaborate on the role of intelligence for the assessment of resilience for both the Israelis and their adversaries. Israel, to a large extent, still followed the conventional offensive paradigm of resisting and repressing terrorist actions rather than enhancing the resilience of their victims as a defensive factor to neutralize or minimize terrorist political gains. Although various security agencies had initiated several new projects to enhance community resilience, the capacity to measure and assess the resilience of the public in general and systems of special national strategic importance in time of crisis in particular was still lacking. The reasons for this included the absence of an accepted methodology, the sensitive issue of whom the responsibility for this unique kind of data collection and interpretation should fall on, as the intelligence community was reluctant to engage in topics that might infringe on domestic politics.

On the social resilience of Israel's adversaries, two challenges for the intelligence community were outlined. The first was to assess the resilience of the political and social systems associated with the core terrorist organizations. The second was to assess the resilience of the general public in the territories of the militant groups. These assessments were vital for counter-terrorist strategies and errors in forecasting responses of the public for the militant leadership could and had been dire. This therefore required an understanding of the social resilience of Israel's adversaries, namely, their society's culture, language and value systems, which was no easy task.

In conclusion, the speaker identified three challenges pertaining to intelligence and resilience. First, high social resilience depended on thorough preparedness, which required a balanced threat assessment that was frequently updated. Second, during an actual crisis, the most important intelligence product was the strategic and tactical early warning needed for both the military and civilian fronts. Messages delivered to the public for this purpose should be trustworthy, clear, succinct and in real time. Third, on the organizational level, it was imperative to ensure the resilience of the intelligence apparatus. This involved the intelligence community recognizing its own vulnerabilities, to foresee the risks it faced and to prepare itself in advance to ensure its full capacity when it was most needed.

RISK ASSESSMENT IN JAPAN

The speaker evaluated Japan's risk-assessment capacity to enhance resilience. In Japan, national efforts to enhance resilience involved local communities, local governments and the private sector. Hence customers of risk assessment were not limited to cabinet members and senior government official but all these stakeholders. Local efforts to enhance resilience employed unclassified strategic risk and intelligence assessments while classified intelligence of specific threats was restricted in its circulation, with non-government stakeholders only on a need-to-know basis. Hence a significant part of enhancing resilience did not involve the use of classified intelligence.

The speaker went on to provide an overview of Japan's approach to risk assessment. The Japanese government conducted separate risk assessments on specific types of hazards but did not conduct a comprehensive risk assessment to compare the priorities of the range of risks. For each hazard, the government conducted a thorough scientific risk assessment and designed risk mitigation measures accordingly. Examples included mega earthquakes, floods, pandemic influenza and missile defence system risk mitigation measures. He noted that it was difficult for the Japanese government to devise a methodology to ascertain acceptable levels of risk for the public. The public's risk perception was dynamic and subject to change, and was influenced by a broad range of variables. Hence the government needed to acknowledge the limits of risk assessment for efforts to enhance resilience.

The speaker pointed out that government resource allocation was significantly impacted by the public's perception of risks. The primary variables determining public trust in crisis managers included the professional expertise of the crisis managers perceived by the public and perceived sincerity of the crisis managers.

Nevertheless, the speaker noted there had been instances of relatively successful risk mitigation, namely, in response to natural hazards. In many instances of earthquakes, the local communities and government had been able to collaborate well to respond to the disaster and prepare for future ones. Evidence of strong community resilience was also noted during the 1995 Tokyo Metro Sarin attack where the majority of casualties were sent to the hospital by fellow civilians at the scene.

The speaker concluded by underscoring the importance of better coordination among the stakeholders, for instance, through establishing two webs of networks—the first among domestic stakeholders and the second with international partners.

DISCUSSION

The panel was asked to elaborate on the various ways where resilience was politicized and whether public support for policy decisions was a necessary feature of a resilient society. A speaker was of the opinion that the critical factor determining resilience at the local and national levels differed. At the local level, leadership was critical to the resilience of the local community while at the national level, a political consensus among leaders was important. Another speaker stated that resilience was politicized as it impacted on resource allocation. Another speaker pointed out that in the case of Japan, the local governments that demonstrated stronger resilience were often those with stronger ties with the local community during peace-time and so received more public support and were also better prepared to respond according to the community's needs. Another speaker argued that before a political strategy for informing the population about vulnerabilities could be devised, there needed to be clarity on what the vulnerabilities were to begin with.

A speaker was asked for his thoughts on the pitfalls of investing in an all-hazards risk assessment that was becoming increasingly popular among many countries, given that Japan did not subscribe to such an approach. In response, he clarified that Japanese political leaders did not necessarily act according to scientific risk assessments in allocating resources and funding. As the culture of stove piping was very strong, each ministry conducted its own risk assessments and worked within its own budget. Moreover, a comprehensive risk-assessment system would cost too much and would likely be deemed unnecessary to achieve the desired ends.

On the issue of monitoring not just domestic resilience but that of adversaries', a speaker noted that it was a difficult task, especially when the adversary's cultural and geopolitical outlooks differed from one's own. Nevertheless, it was a challenge that intelligence agencies had to grapple with because the consequences of an inaccurate assessment could be devastating. Another speaker added that in-depth expertise to develop an understanding and analysis of the threat posed by one's adversary was critical for this purpose.

On the question of whether non-rational thinking, randomness and deception could be quantified, a speaker opined that it was not possible, stressing that a more rigorous approach to risk assessment did not necessarily equate with more quantitative methods as good assessments still relied heavily on human judgments. He added that it was easier to measure quantitatively the impact rather than the causal factors for an event.

FUTURE WORLD ENERGY ARCHITECTURE

The speaker presented on the world energy system and possible scenarios concerning its future development. In his assessment of the present situation, he noted that there were many challenges facing the global economic and trade systems due to several factors, namely that there had been an inevitable shift away from OECD countries to non-OECD countries, especially Brazil, Russia, India and China, which were populous high-growth countries currently gaining economic momentum.

GLOBAL RECESSION, RECOVERY AND THE FUTURE WORLD ENERGY ARCHITECTURE

The speaker began with a brief background on the global energy scene, noting that there had been seven oil price shocks since the 1973 Arab oil embargo. Despite this, there were no serious disruptions to the global energy supply, in a large part due to the role played by the United States and its blue-water navy in ensuring the security of sea lanes.

In his assessment of the present situation, it was noted that there were many challenges facing the global economic and trade systems due to several factors. There had been an inevitable shift away from OECD countries to non-OECD countries, especially Brazil, Russia, India and China, which were populous high-growth countries currently gaining economic momentum. This was coupled with the fact that there had been a lot of uncertainty as to whether the current workings of the economic system with its primary dependence on U.S. consumption and Chinese production would remain as it was.

Turning to the global energy situation, the speaker explained that sustaining a healthy energy system depended on companies being able to generate profits and oil exporting countries being able to balance their current accounts. In order to do so, Saudi Arabia and other OPEC countries estimated that oil had to be priced at USD 75.00 per barrel. This price would not stunt global economic growth and would enable most oil-producing countries, with the exception of Nigeria and Venezuela, to balance their current accounts.

The speaker stated that production in crude oil is estimated to increase to 15 million barrels per day by 2020, fuelled by countries such as Brazil, Russia, Iraq, Nigeria and Kazakhstan. Iraq, in particular, had the potential to challenge the production capabilities of Saudi Arabia. Other countries with unexplored capabilities included Libya and Mongolia. Oil supply would, however, eventually peak and decline although not in the immediate future. The speaker noted that at the price of USD 75.00 per barrel and without too much volatility in oil prices, there would be enough incentive for companies to continue investing in alternatives, including renewable energy alternatives.

The speaker listed seven predetermined elements within the context of the scenarios that he was considering: demographics, hydrocarbon resources, renewable energy potential, low clock speed of renewable energy technologies, the non-linear relationship between energy demand and economic growth, a dual-speed economy and public sector fiscal stress. Regarding hydrocarbon resources, while the belief is that the world was running out of oil, this was not the case yet as supply was still ample. And while the cost of oil production had been increasing, improving technological advances might be able to offset the cost of a particular hydrocarbon. In terms of renewable energy, it was noted that based on a population of 10 billion people, there was potential for renewable energy, such as electric renewable energy, to meet global demands in the long run but not presently. While the potential was already there, this source of energy could not be tapped today due mainly to two reasons: the cost of renewable energy was not low enough to enable it to compete with hydrocarbons and the potential was not equally distributed across geographic regions.

The speaker proceeded to consider the two most divergent scenarios: protectionist and transformative. He opined that while there had been an increase in protectionist tendencies, this was best avoided as globalization had benefited many, including the poor. The aim for most economies should be to make the transition to a path of sustainable re-globalization.

With regard to the regulatory context, he noted that the protectionist scenario would promote an ineffective regulatory environment driven by command-and-control elements whereas the transformative scenario would focus on addressing imbalances, with a collaborative and pragmatic regulatory environment. In terms of demographics, people mobility was an important aspect for both knowledge transfer and economic growth. In a protectionist environment, people mobility would be severely curtailed due to security concerns whereas a transformative environment would encourage student and labor mobility. With regard to innovation, it was stressed that the transformative scenario would sustain more focus on innovation through collaborative endeavors compared to the protectionist environment.

Returning to the issue of achieving a more sustainable environment, the speaker explained that a transformative scenario would mean that energy demands would increase too, as economic growth was likely to be higher. Therefore, there was a need for end-user efficiency to change. He noted that there was now a focus on clean-coal technology across borders, led by a collaboration of countries—including the U.S.—to develop such related technologies at an acceptable price. A protectionist scenario, on the other hand, would cause unsustainable atmospheric carbon dioxide concentrations, which could possibly lead to catastrophic climate change. Even in a transformative scenario, solving the climate conundrum would take time as there would be 10 billion people by 2050 with energy needs which would initially come from fossil fuels before other technologies become usable.

The speaker concluded his presentation by reiterating that the situation within a transformative scenario presented the best possible hope for a sustainable global environment.

PANEL 9

GOING GLOBAL: THE DIVERSITY OF PERSPECTIVES IN ANALYSIS AND FORESIGHT

The panel addressed the extent to which national analytical perspectives, as well as approaches to foresight and risk assessment, are shaped by unique historical, cultural and geopolitical contexts. The two key issues debated were: are such "differences" overdrawn and is there in fact a universal commonality underlying these processes everywhere? Conversely, if the differences are concrete, is there scope for the Eastern and Western analytical communities to nevertheless learn from one another? The discussions covered explorations of the concept of time and its relevance to decision-making.

DIVERSITY IN ACTION

The first speaker explored the concept of time and its relevance to decision making. It was noted that categories and definitions distinguishing the "developed" from the "developing" nation were vague and problematic. The fact of the matter was that diversity existed even within the developing nations.

At first glance and from a temporal perspective, the divide between developed and developing nations seemed clear. The political time horizon for a developed nation like the United States, for instance, was limited to two years and, given the electoral cycle, this was already considered a long horizon. If an incumbent administration tried to make

decisions beyond this time frame, the general concern was that the next administration might be the ones reaping in the benefit.

As such, it placed a limit on the sort of decisions that each administration could make, whereas in countries like India and China, the political time horizons tended to be a lot longer. In the case of India, families could own political parties and their tendency to think about the future consequences of decisions on their future political generations was higher. This was almost the same for China where generational governance was in place.

In the speaker's opinion, developed countries tended to suffer from the "Developed Countries Complacency" syndrome in which they assumed that "they are fine" since their infrastructures were already in place. All that was required was perhaps some fine-tuning or tweaking along the way. In contrast, developing countries either had or were setting up infrastructures that were going to work only for the very first time. Therefore, they made their decisions based on a longer time frame. In the same light, she also noted that developed nations tended to display the same complacency towards peace. While the United States had been at war for about eight years and there was no sense that another country was attacking it on its home ground, the general perception or psychology of most

Americans was that they were essentially living in a time of peace. The Indians, on the other hand, had been fighting wars at their borders since the birth of their nation. This inevitably affected the way urgent decisions were made. For the Indian intelligence service—and for that matter, Israel as well as China—there was an understanding of the importance and urgency of making long-term decisions. This was a perspective that developed nations had, in general, become complacent about.

China's one-child policy, for example, was essentially a long-term natural resource-oriented policy. In an assessment conducted 30 years ago, it was found that China's resources might not be able to sustain a major population growth. The decision was thus made to keep its population size in check. In comparison, the United States adopted a national flood insurance program to cover areas where the market or insurance companies had decided were too dangerous or risky to insure. This resulted in the government stepping in and providing funds for the rebuilding of residential areas each time a flood hit. At the aggregate national level, such a measure would be bound to bankrupt the system. On a broader picture, both policies displayed the flaws that both long- and short-term decisions had on national security.

While it was good to have long-term plans, the speaker stressed that having long-term plans did not necessary mean the plan was any good. The two examples illustrated that bad planning and mistakes were not unique to either the developing or the developed countries. For every case of bad decision made in a developing nation, a similar one could be found in a developed nation as well. One clear example was Dongtan, which had been touted by China as the eco-city of the future. Unfortunately, the location that was chosen for the city was an alluvial island off the coast of Shanghai that sat on a typhoon pathway. This project twinned with the Thames Gateway area in the United Kingdom, which was also a very expensive development based in a flood prone zone.

Finally, in conclusion, the speaker shared with participants a matrix that they could use to understand risk and resilience. The table also measured the ability of countries to make decisions before and after a crisis. Essentially, it was emphasized that from results of the matrix, it was learnt that terminologies like "developing" and "developed" limited the way one interprets things. It would be more helpful to look at the way things were evolving "on the ground".

The second speaker shared his thoughts on the supposed East-West divide, how it affected foresight and the way Asians analyzed events.

He stated that the East-West divide was not easy to identify. From an analysis and foresight perspective, it was opined that many in Asia had not invested in resources that would help them analyze and think more deeply about the future. It might sound like a gap in the way Asians thought about

the future. However, he stressed that it showed a difference in mindset of culture between the systems that could afford to think longer term and those that faced a culture of the guillotine. Thailand and its current administration, for instance, faced more exigencies and immediate security concerns to work out a long-term plan and administer it. This was the case for several societies or governments. As such, they were usually precluded from the culture of foresight as they concentrated their attention and resources on analyzing immediate events.

Secondly, countries that were monitoring Asian affairs tended to focus more on the national and regional issues than Asia's position in global institutions and systems. For example, Asians had been blindsided on issues of climate change and environment degradation. Similarly, for topics on human rights, the speaker mentioned that Asian countries only considered one as important if it had been placed on the global agenda by another country. This also highlighted a major difference in the way things were interpreted. Many perceived that Asia was rising but how this was phenomenal was interpreted among Asians nations very differently. In the last 15 years, the rise of China had been better accepted as part of a greater economic boon by Asians themselves but not by their Western counterparts.

Finally, as a third point, the speaker underlined Asia's rising position in global systems. Thus far, the methodologies for thinking about global issues, institutions and systems had been developed by the West. The same applied for the rules that govern the global systems. This inevitably limited the way Asians thought and how they were perceived in global systems. On this note, he cautioned that this did not suggest that Asians should blindly adopt or reject everything developed by others. Rather, it should be a platform where Asians could try to develop the confidence and the effort to critically examine the rules and institutions in place and, in so doing, build the visions and endurance necessary to start to change systems.

In conclusion, the speaker underscored the importance to remain flexible while thinking or planning ahead. In particular, he noted that the ability to monitor, rethink and adjust was quite fundamental to maintaining the balance between long-term thinking and foresight, and getting things done for issues that matter most at the current time.

The third speaker presented on the factors that shaped South Korea's national analysis perspective. South Korea's national analysis perspective was affected by its history, domestic politics and strategic environment. It was noted that its historical experiences were very much shaped by foreign interventions and internal divisions. The key events that had influenced the way South Korea today viewed external events and affairs were: being under Japanese colonial rule; the period of national liberation and division after World War II; and the Korean War, which divided Korea into the North and the South. This string of historical events

had instilled a siege mentality in most South Koreans in that one constantly felt surrounded or under attack by enemies while harboring a pessimistic view towards major powers in the region.

Domestically, the Military Authoritarian (1961–1986) and Civilian Democratic (1993–present) regimes also had a bearing on the way national analyses and decisions were being made today. Specifically, it was articulated that the level of democratization and the preference of each incumbent political leadership affected intelligence analysis, among other things, in terms of scope, institutional structure and management. It was stressed that domestic politics had a vital role in South Korea's national analysis and, in fact, mattered more than democratization needs.

In a similar light, it was argued that events in the region also influenced the way South Korea positioned itself. Its strategic environment was very much tied to and affected by its antagonistic relation with North Korea. Indeed, North Korea had—since the Cold War era—been viewed as a transnational threat by South Korea. It had to rely on a mix of regional security cooperation, alliances (specifically with the United States) and its own ability to contain it.

All in all, the speaker concluded that strong analyses, foresight and risk-assessment capabilities were crucial for a country's overall resilience and for it to remain robust in the face of both internal and external threats. In South Korea's case, this involved having accurate analyses and assessments of North Korea's current intentions and future plans. In this light, the education and retraining of analysts formed an important part of South Korea's national analytical processes as well as a clear understanding of its historical experiences.

The fourth speaker gave his personal insights on the challenges in making strategic foresight and the factors affecting the way foresight had been treated and utilized by decision makers.

In his opinion, there were two major players in strategic foresight: the heads of intelligence and the decision makers. The heads of intelligence were usually overwhelmed by day-to-day concerns and their perspectives were often shaped by a narrow definition of national security. They were usually the bridge to decision makers and this was advantageous and disadvantageous at the same time. He explained that strategic foresight or information was presented to decision makers if it fit the perception of the heads of intelligence. As for the decision makers, it was stressed that they were first and foremost politicians. It was unlikely for them to invest in strategic foresight beyond their electoral terms or contradicted their visions, mindsets and even images of an existing problem.

A balance between optimism and pessimism was also necessary for strategic foresight. The speaker elaborated that foresight was as much about the uncovering of opportunities as it was about identifying risks. An optimistic mindset was necessary to overcome obstacles and move forward from crises. It was also important for intelligence officers to be self-critical and challenge previous values, experiences and images held of past events. According to the speaker, conceptual mistakes in strategic foresight were often due to a misunderstanding of geopolitical realities and the adversaries' value and culture.

Past values as well as national and personal scars often had a major impact on the way decisions were made. In Israel's case, the Holocaust continued to shape many of its leaders'—and even citizens'—perception of the world. The decisions and policies of former Israeli Prime Ministers David Ben-Gurion and Golda Meir, for instance, were influenced by their personal experiences of anti-Semitism in Europe and the Holocaust. It was stressed that events like the Holocaust and 1948 War of Independence in Israel inevitably shaped the ideologies and values of decision makers and their subsequent treatment of strategic foresight and relationship with their adversaries.

However, perceptions did and could change. In the speaker's opinion, a resilient and robust intelligence or strategic foresight mechanism was one that could challenge the status quo and offer an in-depth analysis of the adversary with an understanding its values, experiences and images of the past. It was mentioned, for example, that Muhammad Anwar El Sadat, former president of Egypt, and Menachem Begin, former prime minister of Israel, were able to depart from their past values and experiences to agree on the Camp David Accord.

It was mentioned that the intelligence community had a much more complicated and difficult role in today's world. The ability to identify trends, processes and events ahead of time were therefore crucial pre-requisites of excellent analysis. For the speaker, the personality of the head of intelligence and the senior officers of intelligence agencies were also central to good analysis and for strategic foresight to make it to the key decision makers. Otherwise, he opined that even the best of analysis would have attracted no readers at all.

In conclusion, the speaker underlined the need for the intelligence officers to maintain their professional integrity and offer decision makers a spectrum of options (both risks and opportunities) to consider for their policies. He reiterated that it was important for the intelligence community to challenge the perception of their leadership towards their adversary. This was a difficult task but he emphasized that it was important to avoid critical mistakes

and challenge existing perceptions of the enemy. Finally, it was noted that, along with the recruitment of the best talents, an organizational culture that champions cultures of openness, integrity and self-criticism—even within the intelligence community—was important for strategic foresight, analysis and decision-making processes.

DISCUSSION

On the concept of resilience, a participant asked how security fatigue could be overcome. It was also mentioned that in many instances a lack of clear directions or over-emphasis on a siege mentality by the state resulted in many not knowing what to expect. A speaker agreed that clear directions and leadership, especially at the governmental level, was crucial for national resilience. The government, nonetheless, would decide which agency should respond and when to do so. In some democratic states, the media also shaped public perception. He added that during the Lebanon war in 2006, the media played a major role in giving vague directions to the public. Several former army generals and commentators were interviewed and their

views broadcasted. As a result of the mishmash of opinions, the Israeli public did not know what was going on. It was much better during the Gaza War—which came later—when the media showed much more self-discipline and the public had a clearer direction as to what was going on. In South Korea's case, a speaker replied that efforts had been made to eliminate the siege mentality and to focus more on the building of self-confidence.

On the question of correlation between globalization and diversity, a speaker responded that the answer or result varied across countries. The correlations could not be generalized. In South Korea's context, globalization had contributed to standardization and broadened thoughts on the region. Another speaker agreed that globalization was a catalyst for diversity. Another speaker added that globalization involved the expansion of relationships that could occur at the personal and national levels. Globalization could also bring about benefits and detriments to both the individual and the state. Another speaker opined that globalization was not necessarily state-led and called for the unpacking of what constituted globalization.

LUNCH KEYNOTE

The lunch keynote focused on how decision makers understood inevitable surprises, where the potential for both progress and disruption was enormous. As such, the speaker suggested that the capacity to anticipate unexpected future shocks would increasingly be a critical aspect of any resilient society.

FOOD FOR THOUGHT

The speaker argued that it was the job of consultants of alternative futures and scenario planning to understand the psychology of decision makers in order to help them make better decisions. Decision makers did not want to see complexity. Hence, the challenge was to understand the complexity and then simplify it. With regard to anticipation, he believed that a good combination of imagination and rigor would allow one to see the near future.

According to the speaker, the long-term future was going to be shaped by the answer to four questions: (i) whether the United States and China could avoid war; (ii) whether long-term growth and prosperity could be achieved; (iii) whether the fruits of that growth would be widely spread; and (iv) whether that growth could be achieved in a sustainable manner. In short, it was important to address whether peace, prosperity, equity and sustainability were within reach. An affirmative answer to all the four questions would result in a positive scenario while a negative response to

any one of the questions would pose a problem. These four factors were the core risks that needed to be dealt with and prevented.

On the issue of recognition, the real key was in assessing which of the environments decision makers were actually confronting: whether it was a world of normal dynamics where the rules of the game were relatively stable; one that changed slowly, allowing decision makers to act with confidence in the face of their own experience; or one where they faced a time of crisis where rules were very open to change and the past was not a good guide to decision making in the new future.

Referring to preparation, the speaker talked about how UPS was a good example of preparation at its best. During the recent volcanic disruption in Europe, when air traffic was adversely affected, it was business as usual for UPS. Even though UPS was not prepared for a volcanic eruption, it was prepared for an outbreak of disease that could cause disruption to air traffic in different parts of the world. As a result, they adapted the software and contingency plans for such an outbreak to the volcanic disruption to air traffic. He argued that this supported the point that the consequences of the events rather than the events themselves were more important, as many events produced similar consequences, and thinking about consequences maximized resilience and flexibility.

To conclude, the speaker remarked that though the world was faced with the possibility of a major catastrophe, a half century of war and recession in the near future, he was confident that the four optimistic outcomes for the future—avoiding war, ensuring prosperity, equity and sustainability—were achievable in the long run.

DISCUSSION

On whether there was an optimum number of scenarios and perhaps a range of probabilities that would be recommended for intelligence products, the speaker was of the opinion that a minimum of two (also the optimal) and no more than four was ideal. He also warned against including probabilities in scenarios because it would give the decision maker the opportunity to opt out of scenarios with lower probabilities, which was one of the most common mistakes one could make.

The audience wanted to hear the speaker's views on issues of gradual change as opposed to short-term shocks or major long-term changes. He replied that the reality was that we constantly saw forces that changed the environment over time in ways that we might not have imagined, for instance, mobile communication, which had dramatically transformed the world. That change, over the course of about 20 years, had been shaping the global environment in fundamental ways. Hence, not only was there a need to identify big dramatic scenarios of change but there were also gradual, inexorable (predetermined in many ways) ones that would ultimately accumulate into a rather radically different environment.

CONFERENCE PROGRAM

Day 1
Sunday, 12th September 2010

0830h — **Arrival of invited foreign participants and speakers**

0830-1815h — **Conference Registration**

1400-1600h — **GFF Steering Group Meeting**

1900-2100h — **Evening Welcome Reception**

Day 2
Monday, 13th September 2010

0830-900h — **Welcome Remarks**
David I. Adelman, United States Ambassador to Singapore
Eddie Teo, Chairman, Board of Governors, S. Rajaratnam School of International Studies, Nanyang Technological University

0900-0930h — **Opening Address**
Professor S Jayakumar, Senior Minister and Coordinating Minister for National Security, Singapore

0930-1000h — **Break and Networking**

1000-1015h — **Introduction to GFF General Meeting**

1015-1200h — **Panel 1: Looking Out for Future Shocks**

1200-1330h — **Lunch Keynote: Resilience: Defying Terrorism and Mitigating Natural Disasters**

1330-1500h — **Panel 2: Resilience in the Face of Future Shocks**

1500-1530h — **GFF Discussion: GFF New Directions**

1530-1600h — **Break and Networking**

1600-1715h — **Panel 3: Futures Thinking in the Singaporean Government**

1715-1730h — **Wrap-up of Day 2 and Plan for Day 3**

1900-2100h — **No-host Communities of Interests (COI) Dinners**

Day 3
Tuesday, 14th September 2010

0830-1000h — **Panel 4a: Practice and Organization of Intelligence/Radicalization and Counterterrorism: Addressing Emerging Forms of Terrorism**

Panel 4b: Launching of the Human and natural Resources Security COI

1000-1030h — **Break and Networking**

1030-1200h — **Panel 5a: Illicit Trafficking COI: Emerging Challenges in Illicit Trafficking**

Panel 5b: Emerging Disruptive Technology COI: Report on Cyber-Security and Disruptive Technology

1200-1345h — **Lunch Keynote: Is Resilience an Intelligence Issue?**

1345-1515h — **Panel 6: Strategic Foresight and Warning COI: Can Foresight be Actionable Today?**

1515-1545h — **Break and Networking**

1545-1715h — **Panel 7: Looking Ahead to a GFF Research Program: Cross-cutting Issues**

1715-1730h — **Wrap-up of Day Three**

1900-2100h — **Dinner Keynote: Developing the Resilient, "Relational" State: From Government to the People to Government with the People**

Day 4
Wednesday, 15th September 2010

0830-1000h   **Panel 8a: Organizing Intelligence for Resilience**

                            Panel 8b: Global Recession, Recovery and the Future World Energy Architecture: Scenarios to 2030

1000-1030h   **Break and Networking**

1030-1200h   **Panel 9: Going Global: The Diversity of perspectives in Analysis and Foresight**

1200-1400h   **Lunch Keynote: Food for Thought**

1400-1410h   **Conference Round Up**

1410-1630h   **GFF Business Session**

ABOUT THE GLOBAL FUTURES FORUM (GFF)

What is GFF?

The Global Futures Forum (GFF) is a multinational, multidisciplinary intelligence community that works at the unclassified level to identify and make sense of emerging transnational threats. Its primary goal is to foster the collaborative development of insight and foresight through the exchange of different perspectives among its members.

Who is GFF?

GFF seeks to involve a diverse population of officials and subject-matter experts in order to stimulate cross-cultural and interdisciplinary thinking, and to challenge prevailing assumptions. Core members in intelligence and security organizations are joined by selected experts from academia, non-government organizations, and industry. There are currently upwards of 1500 GFF individual participants from over 40 countries.

How does GFF work? GFF works through face-to-face meetings
- Full membership meetings: 2005 Washington (Airlie House); 2006 Prague; 2008 Vancouver
- Singapore will host the full membership meeting in 2010
- Community of interest (COI) workshops: smaller, topic-based meetings held regularly

On the Web: www.globalfuturesforum.org

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

ABOUT THE CENTRE OF EXCELLENCE FOR
NATIONAL SECURITY (CENS)

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

Why CENS?

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

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

What Research Does CENS Do?

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

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

Radicalisation Studies

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

Social Resilience

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

Homeland Defence

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

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

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

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

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

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

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

ABOUT THE S. RAJARATNAM SCHOOL OF
INTERNATIONAL STUDIES (RSIS)

The **S. Rajaratnam School of International Studies (RSIS)** was officially inaugurated on 1 January 2007. Before that, it was known as the Institute of Defence and Strategic Studies (IDSS), which was established ten years earlier on 30 July 1996. Like its predecessor, **RSIS** was established as an autonomous entity within Nanyang Technological University (NTU). **RSIS**' aim is to be a leading research institution and professional graduate school 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, international political economy, diplomacy and international relations
• Collaborate with like-minded schools of international affairs to form a global network of excellence

Graduate Education 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 (M.Sc.) 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). Teaching at RSIS is distinguished by its focus on the Asia-Pacific region, the professional practice of international affairs and the cultivation of academic depth. Over 180 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 endowed 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 an **RSIS** priority. **RSIS** maintains 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 about RSIS, visit
http://www.rsis.edu.sg.

ABOUT THE NATIONAL SECURITY
COORDINATION SECRETARIAT (NSCS)

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 Senior Minister Professor S. Jayakumar.

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 organises 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 centre 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.

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

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

PONDER THE IMPROBABLE