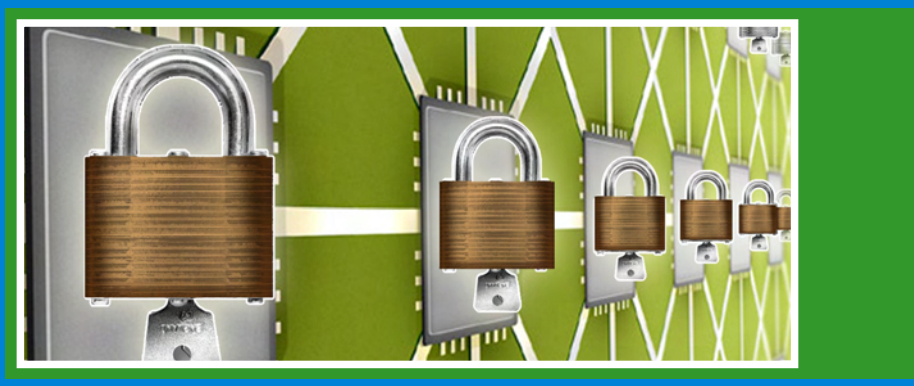

NETWORKED GOVERNMENT & HOMELAND SECURITY WORKSHOP

CONFERENCE REPORT

7 JANUARY 2008
SINGAPORE

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

NATIONAL SECURITY COORDINATION SECRETARIAT

NETWORKED GOVERNMENT & HOMELAND SECURITY WORKSHOP

CONFERENCE REPORT

REPORT ON A WORKSHOP ORGANIZED BY
THE CENTRE OF EXCELLENCE FOR NATIONAL SECURITY (CENS)
AT THE S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES (RSIS),
NANYANG TECHNOLOGICAL UNIVERSITY, SINGAPORE
WITH THE SUPPORT OF
THE NATIONAL SECURITY COORDINATION SECRETARIAT (NSCS)
AT THE PRIME MINISTER'S OFFICE, SINGAPORE

7 JANUARY 2008
SINGAPORE

S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES,
NANYANG TECHNOLOGICAL UNIVERSITY

CONTENTS PAGE

EXECUTIVE SUMMARY

On 7 January 2008, the Centre of Excellence for National Security (CENS), with the support of the National Security Coordination Secretariat (NSCS), organized the Networked Government and Homeland Security Workshop at Marina Mandarin Hotel, Singapore. The workshop looked at the issue of networked governments in the context of homeland security and brought together a mix of international and local academics and practitioners to share both current research as well as best practices.

Sometimes termed "whole-of-government", the drive for a networked government arose out of the recognition that many of the issues and problems governments must deal with cannot be handled by a single agency. Whether they are so-called "wicked problems", such as religious or racial intolerance, radicalization and poverty, or new trans-national threats like terrorism or pandemics, or because dealing with the response and recovery efforts in the aftermath of a crisis (whether manmade or natural) requires many agencies to work together in a coordinated fashion, the issue of a networked government is extremely pertinent. The Networked Government and Homeland Security Workshop attempted to broadly sketch out the contours of this topic. The morning session focused on looking at networked governments from a broad, multidisciplinary perspective. Brint Milward discussed some of the problems managers face, both in managing a network and in managing within a network. Verna Allee gave the attendees a perspective from the corporate world on the use of what is called "value networks" and the use of value network analysis in corporations.

During lunch, the workshop was privileged to hear from Ambassador Lam Chuang Leong, who gave a highly original talk on how the development of a networked government in Singapore—and its future—is related to differing types of innovation. Ambassador Lam discussed the necessity of introducing a new innovative mindset, one that calls for exploiting the distributed knowledge, information and intelligence in the population at large, in finding new connections and opportunities.

The afternoon session focused more clearly on homeland security topics as they relate to this issue. Brian A. Jackson discussed the implications for governments of the terrorist use and the development of new technologies that enable them to organize in a networked fashion. Donald Moynihan examined case studies of disaster and crisis response in the United States and the use of Incident Command Systems as one way that the power of networks could be effectively harnessed. Complementing this presentation, Derek Pereira presented on Singapore's Homefront Crisis Management and how such a framework goes beyond just managing civil-security and civil-defence incidents and adopts an all-hazards approach that prepares the homefront to deal with any issues that may arise.

WELCOME REMARKS BY DIRECTOR, NSCC

Mr Lee Ark Boon, National Security Co-ordination Centre

In his welcome remarks, Lee Ark Boon highlighted the importance of a networked-government approach to mitigate current and future challenges to homeland security. Firstly, as networks of trans-national and criminal groups are becoming more intricate, no single government agency has all the requisite expertise and knowledge to tackle these problems alone. Secondly, a dynamic and resilient response by a network of agencies, working together with the private sector and ordinary citizens, would be required to mitigate national crises.

While the need for such an approach is generally evident, Lee underscored a key obstacle that organizations need to address: the inertia of evolving from a "need-to-know" to a "need-to-share" paradigm. Recent security challenges necessitated reviewing the structures, processes and measures in place that enable Singapore to anticipate, plan for and deal with crises. This workshop is nevertheless timely, as effective strategies for securing the nation entail constant innovation and the sharing of fresh perspectives.

MORNING SESSION

Best Practices and Tools for Public Management Networks

Managing in Networks

Prof. Brinton Milward, University of Arizona

In his presentation, Brint Milward explored ways to mitigate the challenges of managing a network and managing in a network. Unlike a bureaucracy that is modelled on a structured command-and-control paradigm, networks are more nebulous as they are based on relationships. As a result, most governments will only adopt a networked approach as a last resort to supplement the limitations of the bureaucratic model. However, the creation of effective networks require the breaking down of silos, a difficult task because of varied commitments to network goals, culture clashes, turf issues, loss of autonomy, the lack of a chain of command, coordination costs, reduced accountability and the loss of proprietary knowledge. Hence, governments adopting a networked approach should have clear and realistic expectations of what they hope to achieve from it.

Milward pointed out that approaches to managing a network vary with the nature of its governance structure. The most common is the self-governed network, which emerges as and when the need arises and is characterized by a consensual decision-making process.

At times, self-governed networks may evolve into one with a lead agency coordinating the rest. Another type is a networked administrative organization specifically set up to manage a network. He stressed that, regardless of the network type, there is a practical need to ensure a mechanism is in place to determine whose views should prevail in the absence of a consensus.

Milward proceeded with identifying five key aspects of network management. Firstly, accountability in networks could be managed by (i) monitoring one's organizational involvement, (ii) ensuring that dedicated resources are used for network activities, (iii) ensuring that credit is given for network activities and (iv) resisting efforts to "free ride". Secondly, conflicts in networks can be mitigated by working (i) to resolve differences with other network member organizations, (ii) to resolve differences between network leaders and (iii) to work within one's organization to strike a balance between its needs and those of the network. Thirdly, the management of design involves (i) working with partners to maximize the potential of the existing work structure, (ii) creating a better structure with incentives that reward cooperation and (iii) accepting that network effectiveness requires shared decision-making among the partners. Fourthly, the commitment to networks can be enhanced by institutionalizing network involvement so that support for network goals is widely shared within the organization. Lastly, legitimacy can be reinforced by (i) demonstrating to members and stakeholders the value of participation, and (ii) legitimizing the role of one's organization in the network.

In conclusion, Milward emphasized the need for "relationship budgeting" in the managing of a network. While conventional wisdom dictates that "more is better", he cautioned that connecting broadly with many partners would require a lot more resources and time, running the risk of overwhelming the ability of members to actively participate in the network. Hence a "less is more" approach that strategically reduces overall ties by creating fewer links decreases redundancy, increases diversity and frees up more time and resources would be more efficient.

Value Networks and Complex Adaptive Organizations

Ms Verna Allee, Value Networks LLC

Verna Allee discussed the emerging use of "value networks" in the corporate world and their possible application in the field of national security. Allee defined a value network as "any purposeful organization or network that engages in complex dynamic exchanges of tangible and intangible value to create social or economic good". This type of network analysis differs from traditional social network analysis in many ways, which Allee argued, only shows social relationships and interactions but not typically business processes.

On the other hand, value network analysis aims to show whole systems (including people), knowledge flows and processes. It puts people and their roles at the centre of the action (rather than relationships). More importantly, Allee argued, it shows how knowledge and other intangibles create value and can reveal dependencies in one's business transactions.

In doing so, it can allow one to evaluate the performance of a network, the roles that support it and the conditions that are critical in the functioning of the network.

Allee presented new insights into how value networks foster innovation at the regional level in Europe, the industry level in transportation and technology, and at the business level in a variety of industries. Allee then demonstrated how Boeing used value network analysis to achieve a six-fold productivity increase in Flight Test and Validation for the latest 787 Dreamliner aircraft. Lastly, Allee showed how other companies, such as Cisco, Telenor, SAP, Mayo Clinic and Kimberly-Clark, as well as government agencies and global action networks, are using the network perspective to expand capabilities, build sustainable relationships and deliver sharp performance improvements.

DISTINGUISHED LUNCH ADDRESS BY AMBASSADOR LAM CHUAN LEONG

Future Challenges of Networked Government in Singapore

Ambassador Lam Chuan Leong, Ministry of Foreign Affairs

Networked government in Singapore, according to Ambassador Lam Chuan Leong, evolved over the last decade or so in response to increasing complexity in government and government services. Initially, the key driver was the programme to introduce e-government. Ambassador Lam then went on to discuss how the development of networked government in Singapore—and its future—is related to differing types of innovation. In this regard, Ambassador Lam distinguished between two types of innovation: "extrapolative" and "generative".

The former is at the heart of most of the initiatives undertaken by government because of its success in using expert knowledge to identify and solve known problems and public needs. Singapore's success in public service delivery and "making things work" has won many international accolades.

The latter type of innovation, on the other hand, is required to address future unknown threats or opportunities. This is because unknown threats and opportunities, such as emergent epidemic diseases, natural disasters and human terrorist threats, are characterized by "uncertainty" and are not amenable to approaches based on extrapolative innovation.

"Uncertainty" is taken to mean a future event whose nature and probability are unknown. Uncertainty is therefore different from "risk", which refers to the possible occurrence of an uncertain but known event that can be measured by some a priori probability distribution.

Extrapolative innovation, as it depends on prior knowledge, is not particularly suited for the task of anticipating risks or future unknowns. This is better done through an approach that harnesses the diversity and knowledge of many people.

Matters steeped in technical knowledge are best left to expert judgment. The value of expert opinion is, however, of little worth for threats that emerge with no prior patterns or with very weak precedents. For such cases, the distributed knowledge among the population at large is more effective in detecting and understanding such an emergent threat. Ambassador Lam cited the Iowa Electronic Options Market and Wikipedia as examples of this.

The value of collaborative efforts in information sharing can be seen in the handling of the SARS epidemic. Initially, the Chinese authorities released little information, thinking perhaps that it would be best solved locally—without publicity. Localized infections could perhaps be treated in this manner but SARS was a new infection that spread too fast to be contained this way. Given the trans-national threat that this disease posed, the authorities in China and elsewhere found that the only way to curb its progress was to depend on worldwide collaboration and sharing of information and research.

Singapore contributed to the collaborative effort by proposing the use of thermal imaging to detect high fever at airports and other checkpoints. These equipment and technology were not developed for SARS in the first place. This illustrates the value of collaboration in making a connection between two disparate pieces of information: the fever symptom of SARS and the capability of thermal imaging.

To address such changes in the types of threats that states must deal with, a new mental model of innovation is necessary; it is one that calls for exploiting the distributed knowledge, information and intelligence in the population at large, in finding new connections and opportunities. It calls for the connecting of silos, of working collaboratively and avoiding the use of too much ex-ante judgment.

The challenge ahead lies in introducing this new mindset and integrating it into an organization that is strongly wedded to the use of extrapolative innovation, such as the civil service. Ambassador Lam, however, concluded that Singapore has been able to come up with very novel breakthrough solutions, typical of generative innovation in its past. The challenge in future is to keep up this record.

AFTERNOON SESSION

Network Approaches to Homeland Security & Crisis Management

Technology and the 'Networked Terrorist Threat:' Implication for Whole-of-Government Responses

Dr Brian Jackson, RAND Corporation

Brian Jackson spoke on the use of technology by terrorist groups and the threats they could pose to modern societies. Terrorist groups that are effective in using new weaponry technology could pose a more potent threat than those that are not. Additionally, understanding the full range of issues and organizational behaviours associated with terrorist groups' use of technology is critical for the crafting of effective counter-terrorism policy, the choosing of appropriate response options and the design of defensive measures.

There are several technologies that terrorist groups might try to acquire, ranging from simple information-sharing tools to radiological or nuclear weapons. These technologies could be acquired through purchase, technology sharing among groups and internal "research and development" within terrorist cells and networks. Jackson added that acquiring new technologies takes more than just sourcing and purchasing new hardware. Expertise is needed to utilize them effectively and efficiently.

Therefore, the study of knowledge acquisition is just as important as that of technology usage by terrorists. The magnitude of threats from terrorist usage of technology depends on their "technological know-how". In essence, the threat that "technologically-equipped" terrorist groups might pose depends on both their intentions and their capabilities for using such technology effectively.

The range of technological tools and solutions available to terrorist groups are not restricted to bomb making or improvised explosive devices (IEDs) alone. According to Jackson, network technologies include a wide array of information-based technologies and could be used to refer to: (i) consumer oriented technologies that store, manipulate, communicate and display information; and (ii) devices that the military would label as command, control, communications, computers, intelligence, surveillance and reconnaissance technologies.

Technology can help terrorists bridge coordination and communication gaps at different stages of their attack plans. The mobile phone, for example, can be used for communication, coordination and weapon triggering purposes during the recruitment, resource acquisition, intelligence gathering and the actual attack phases. Likewise, terrorist groups make use of commercially available consumer products such as portable video cameras and Internet-enabled laptops to capture, share and disseminate information.

A study conducted by RAND in assessing the impact of network technologies on terrorist activities found that a limited number of technology enablers do have the potential to produce major changes in the dynamics between security forces and terrorist groups. However, most technological enablers provide only an incremental improvement or perform solely supportive functions to most terrorist operations. Essentially, the key finding is that network technologies can provide some advantages to terrorist organizations but they are evolutionary rather than revolutionary in many cases. Moreover, while the Internet and other publicly available sources of information can be used to gather information to support attack planning, critical information is usually not readily available on such media and requires real physical pre-attack surveillance instead.

In conclusion, Jackson noted that, while there are indications that terrorist groups are interested and actively pursuing new technologies, the threat still depends on how capable they are in adopting and using new technology effectively. Finally, terrorist responses to defensive technologies have to be considered. Jackson reasoned that the effectiveness of defensive technology would depend on the terrorist groups' ability to counter or deflect it. As such, strategies could be developed to both identify and address areas where these groups could derive information and, as a result, improve their abilities to circumvent defensive technologies.

Crisis Management in the Homefront

Mr Derek Pereira, Ministry of Home Affairs

Derek Pereira started by emphasizing that Homefront Crisis Management (HCM) is an endeavour fraught with challenges today. Not only do states face a myriad of threats, homefront crises can also occur suddenly and potentially paralyse society within a short timeframe. Moreover, these crises can run the whole spectrum of intensity and resource deployment, from a localized incident of limited consequence to one where national survivability is at stake. Depending on the scale and complexity of the crisis, the amount of resources required to deal with it effectively can span the resources of a few agencies to that of the entire country. This situation poses its own set of problems, as there is usually inherent unevenness in extant homefront capabilities. Given these issues and challenges, Pereira argued that it is imperative that states adopt a whole-of-government approach towards HCM. In particular, all relevant agencies must work together in an established framework, with seamless communication and coordination—and sometimes in unconventional roles—to manage the crisis.

Pereira went on to elaborate on the evolution and development of Singapore's HCM model, noting that the SARS episode in 2003 had been an institutional watershed. Prior to the SARS crisis, the Executive Group (EG)—the key executive body charged with managing peacetime crises in Singapore—focused mainly on scenarios that were civil security or civil defence in nature, such as building collapses or bomb blasts. These scenarios were typically conceived to be managed by a single incident manager, supported by various agencies but without requiring a specific and deliberate multi-agency structure to handle the indirect ramifications arising from an incident.

But following the strategic surprise of SARS in 2003, policymakers realized that, because national crises can come in unexpected forms, just solely relying on the prevailing HCM structure is not enough. More that that, what is required is a comprehensive crisis-management framework that transcends just managing civil-security and civil-defence incidents and to adopt an all-hazards approach that prepares the homefront to deal with any possibility. Indeed, such a framework should include a mechanism for seamless integration at both the strategic and operational levels among the various government agencies to tackle any crisis at hand.

To this end, Singapore has revamped its HCM framework to create a more multi-dimensional and robust management structure. At the strategic echelon,

there are the Homefront Crisis Ministerial Committee (HCMS) and the Homefront Crisis Executive Group (HCEG). The former provides overall strategic and political direction while the latter supports the HCMS through inter-agency policy guidance for both peacetime contingency planning as well as operational coordination and consequence management during a crisis. At the operational level, there are various functional inter-agency crisis management groups with specific responsibilities and tasks; this structure integrates the various government crisis-management sections. Finally, at the tactical level, there are the crisis and incident managers who oversee direct operations and coordination at the service-delivery level. Pereira stressed that the strength of the revamped HCM paradigm lies in its embedded inter-agency linkages and processes that ensure quick, holistic and coordinated response and execution. This was clearly evinced by the effectiveness of the crisis management groups during the SARS crisis.

Pereira also made clear that having a more collaborative, nimble and responsive HCM architecture is not the end game: having a useful institutional structure does not flawlessly translate into a solution that ensures all government agencies work together in a coordinated manner. Just as important is the need to stay vigilant and be adequately prepared for crises. Comprehensive exercises should therefore be regularly conducted to test the readiness and robustness of the HCM structure, taking care to ensure that lessons learnt from these exercises would be drawn to fine-tune the prevailing model.

Pereira concluded his presentation with a qualifying but nonetheless pertinent remark. While he was confident that the current HCM model works, worldwide experiences have reflected that all systems built to handle crises, which, by their nature, are very unpredictable, are always evolutionary. That said, he is also sure that Singapore is on the right track, using fundamentally sound principles in a flexible framework for a multi-networked response.

The Use of Networks in Crisis Response: Examining Incident Command Systems

Associate Prof. Donald Moynihan, University of Wisconsin-Madison

Donald Moynihan began his presentation with a brief account of the evolution of the Incident Command Systems (ICS) in the United States. The idea of the ICS in the United States, according to Moynihan, started in the 1970s when fire responders in California wanted a common operational working set of language, concepts and communications. The need for a common operating page led these responders to institute a centralized response authority to coordinate their actions. When the reputation of California's centralized fire response model grew, other states soon followed suit and adopted similar systems. Eventually, in 2004, the ICS became a mandatory institutional requirement for crisis responders in the United States.

Moynihan noted that the traditional understanding of the ICS in crisis-management literature was that of a hierarchical set-up, one that entailed a command-and-control structure. Such a perspective, however, does not take into adequate account the implications and realities of an increasingly "networked" crisis milieu, whereby response typically relies on consensual and collaborative action by multiple parties and responders in an inter-related web. Yet, reliance on network lenses to solely understand the crisis response landscape is also equally unsatisfactory, for such paradigms often do not given enough credit to the utility of centralization. Given these theoretical limitations, Moynihan argued that there is a need for a mental shift: to move the debate beyond the current "hierarchy versus network" dichotomy and to recognize that it is in fact possible—and indeed, desirable—to combine both a centralized approach to coordinating multiple agencies while

acknowledging the complexities created by the networks. Moynihan termed this the "network governance" approach.

To shed further light on the dynamics of governance within networks, Moynihan examined six case studies of ICS in the United States: wild land-urban fires in California (both in 1993 and 2003); terrorist attacks in Oklahoma City (1995) and the Pentagon (9/11); animal disease outbreaks (2003); and Hurricane Katrina (2005). The findings from these case studies suggested that centralized administration of networks yielded a number of key benefits. First, it meant that the response system shared a common communication platform and network-governance rules. Second, the central governing organ served as a useful mechanism to mediate and resolve potential conflicts as well as to coordinate tasks to avoid duplication or absence of response. Third, the governing organ was also the central point through which information flowed. This speeded decisions and clarified accountability.

Still, even with these central governance "perks", Moynihan noted that a number of network effects ineluctably impacted the crisis-response management. For one, there was the influence of network diversity. Larger and more diverse ICS found it difficult to coordinate actions and mediate tensions that existed between actors from different organizations. At the same time, incorporating emergent aspects of the network during crises was problematic.

Then there was the problem of shared authority. Command authority was frequently ambiguous and this meant that authority was often negotiated or contested between members. But more than that, because every single commander tended to focus, somewhat parochially, on attending to the priorities and concerns of their respective agencies first, there existed an unhealthy potential for competing and inconsistent commands.

Finally, there is the issue of trust. Insufficient levels of trust among members brought about gratuitous network friction that affected crisis-response effectiveness. There was a higher propensity for blame shifting, solo action, information and resource hoarding, and conflict over authority and policy. With these in mind, Moynihan emphasized that trust among members in a network must be an essential supplement to command relationships.

Moynihan concluded by suggesting four policy recommendations for consideration:

1. It is important to clarify the basis for command. While the ICS is a command structure, the structure itself does not indicate who is in charge. The command relationships need to be better delineated.

2. Given the variety of backgrounds of different actors in the network, it will be desirable to enhance the ICS knowledge baseline of the members. These can be achieved via regular coordinated training.

3. There is a need to build and maintain working relationships between crises—not just during crises. While it is possible to foster trust during crises if the actors perceive themselves as part of a shared effort with reliable partners, trust can also collapse in a crisis if network members perceive each other as failing. A more durable basis for trust would be to nurture and sustain working relationships between crises.

4. Emergent aspects of the network, such as new civil actors, can be better incorporated through pre-identification, advance role planning and training exercises.

ROUNDTABLE DISCUSSION

Participants at the Roundtable Discussion

The first question posed during the roundtable discussion involves the value of adopting a network approach as opposed to continuing with "business as usual".

One respondent answered that it is not clear if networked governance is superior to centralized governance with regard to homeland-security issues. It depends on the severity of the problem you are dealing with. There is a contingency relationship between the degrees of severity of the problem you are facing and the nature of the network you would create to respond to it. For example, if one is looking at limited incidents, such as fighting wildfires, the Incident Command System in use in America is very hierarchical, with a few network elements to it. What is critical in this area is the need to move away from the notion that there are "ideal types" of organizational form. In reality, most of the kinds of things we call "networks" in the world are an admixture of different organizational forms, such as market and hierarchy.

A second response to this question was that one of the needs for a network is that the policy area is not covered by the capabilities or authority of one agency. In terms of homeland security, this covers, at least in the United States, a vast policy space. It may be the case that because "homeland security" covers such a broad policy space that networks are needed. But one can flip that problem on its head by saying that the homeland-security policy space has been self-defined as such and so it is not clear if all those organizational pieces necessarily need to be together.

Another respondent answered that discussions of social networks almost always perceive them as benign, positive entities. But today's discussions have shown the importance of purpose in examining networks. Many have negative tasks they seek to achieve. Research has also shown that even if networks have a positive purpose—crisis response, healthcare delivery—they do not always succeed. Secondly, in the academic literature, there is a tendency to examine networks as an ideal type. There is a lot of variation between network types and one must be specific in discussing the type of network governance system that is in place. Finally, even with very centralized networks, there are problems of trust and shared authority that must be explored.

The question was then asked on the role of networks in post-crisis recovery efforts. A speaker noted that the nature of networks could change over time. Crisis-recovery networks may differ from crisis-response networks, as the former can a require different set of actors and may be less hierarchical than the latter.

An audience member noted that while there is a desire for nimble, flexible networks, human instinct is to move such a network into a rigid structure, with doctrines, standard operating procedures (SOPs), and so on. How does one then ensure flexible, nimble networks that are resilient and adaptive, while keeping at bay the human tendency to meddle and construct rigid organizations?

A speaker noted that while human nature may tend us towards creating hierarchies, it is also something that people are trained to think and act in. The speaker noted that there have been shifts in the business world with regard to how management is conducted, whether it is innovations such as a focus on process, or the role of teams in organizations. Indeed, bureaucracy was at one time a new idea. However, an enormous amount of education is required to teach people these ideas, and how to make them work within such a system.

As such, there needs to be a comparable training focus on the ideas, language and the tools of networks.

One speaker agreed on this point, noting that when Frederick Taylor's book, Scientific Management, came out there were congressional hearings accusing him of communism and it was thought to be a terrible idea. For network governance, a similar educational approach, like what has been done in management studies, needs to be taken, including training programmes, diffusing curricula, best practices, case studies and advanced education.

However, one speaker questioned the premise of the question posed, noting that SOPs can be incredibly useful as a way to accumulate and disseminate knowledge in order to avoid reinventing repeatable tasks. There is a large organizational-learning challenge in bureaucracies as well as networks and there is a need to understand where SOPs help, and where they have become simply "red tape" that impedes learning and flexibility.

The question was then asked of how one builds trust and reciprocity within network governance so that the network will function effectively, especially in a crisis.

A response was that one cannot force trust to exist, but the sort of behaviours that will ensure trust can be negotiated. However, cultural differences may affect expectations and this issue needs to be discussed in a results-focused manner, as it is something that global corporations face.

Note: "Chatham House" rules were applied for this discussion so as to enable for a free-spirited and creative dialogue; discussants are thus not named in this report.

Rapporteurs:
Yolanda Chin, Hoo Tiang Boon, Nirupema Kishav, and Ng Sue Chia

Edited by:
Greg Dalziel and Kumar Ramakrishna

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

WORKSHOP PROGRAMME
7 JANUARY 2008

Practices and Tools for Managing in Public Networks

0915 Welcome Remarks by Lee Ark Boon

0940 H. Brinton Milward, "Managing in Networks."

1020 Q&A Chaired by Asst. Prof. Terrence Lee, RSIS

1030 Coffee/Tea Break

1045 Verna Allee, "Value Networks and Complex Adaptive Organizations."

1120 Q&A Chaired by Asst. Prof. Norman Vasu, RSIS

1130 Distinguished Lunchtime Talk by Ambassador Lam Chuan Leong, "Future Challenges of Networked Government in Singapore."

1215 Q&A Chaired by Assoc. Prof. Kumar Ramakrishna, Head, CENS

Afternoon Session – Network Approaches to Homeland Security and Crisis Management

1330 Brian A. Jackson, "Technology and the 'Networked Terrorist' Threat"

1415 Q&A Chaired by Asst. Prof. Bernard Loo, RSIS

1425 Derek Pereira, "Crisis Management in the Homefront"

Donald Moynihan, "The Use of Incident Command Systems."

1525 Q&A Chaired by Asst. Prof., Bernard Loo, RSIS

1540 Coffee/Tea Break

1600 Roundtable Discussion

1700 End of Workshop

LIST OF SPEAKERS / MODERATORS / PARTICIPANTS

1. Mr. Lee Ark Boon
   Director
   National Security Co-ordination Centre
   Singapore

2. Professor H. Brinton Milward
   Providence Service Corporation Chair in Public Management
   Associate Dean and School Director
   Eller College of Management
   University of Arizona
   United States of America

3. Ms. Verna Allee
   Chief Creative Officer
   Value Networks LLC
   United States of America

4. Dr. Brian A. Jackson
   Associate Director
   Homeland Security Program
   RAND Corporation
   United States of America

5. Mr. Lam Chuan Leong
   Ambassador-at-Large
   Ministry of Foreign Affairs
   Singapore

6. Mr. Derek Pereira
   Director
   Security Plans/Development Directorate
   Homefront Security Division
   Ministry of Home Affairs
   Singapore

7. Associate Professor Donald Moynihan
   La Follette School of Public Affairs
   University of Wisconsin-Madison
   United States of America

8. Associate Professor Kumar Ramakrishna
   Head Centre of Excellence for National Security
   S. Rajaratnam School of International Studies
   Singapore

9. Assistant Professor Terence Lee
   S. Rajaratnam School of International Studies
   Singapore

10. Assistant Professor Norman Vasu
    S. Rajaratnam School of International Studies
    Singapore

11. Assistant Professor Bernard Loo
    S. Rajaratnam School of International Studies
    Singapore

12. Christina Ong
    Assistant Director
    Security Development Branch
    Ministry of Home Affairs
    Singapore

13. Anna Lee
    Assistant Director
    Security Plans Branch
    Ministry of Home Affairs
    Singapore

14. Major Taharudin Piang Ampatuan
    Associate Research Fellow
    International Centre for Political Violence and Terrorism
    S. Rajaratnam School of International Studies
    Singapore

15. Benjamin Lee
    Senior Associate
    Budget Policy Unit
    Ministry of Finance
    Singapore

16. Lim Tuan Liang
    Assistant Director
    Strategic Development
    Ministry of Home Affairs
    Singapore

17. Roger Wong
    Assistant Director
    National Security Co-ordination Centre
    Singapore

18. Alan Chow Mun Keong
    Assistant Director
    Operations Management & Readiness Branch
    Ministry of Home Affairs
    Singapore

19. Leong Ming Wei
    Assistant Director
    National Security Co-ordination Centre
    Singapore

20. Ni De-en
    Assistant Director
    National Security Co-ordination Centre
    Singapore

21. Jace Goh
    National Security Co-ordination Secretariat
    Singapore

LIST OF SPEAKERS / MODERATORS / PARTICIPANTS

22. Professor Ori Sasson
Singapore Management University
Singapore

23. John Lim
Deputy Director
Security Plans/Development Directorate
Ministry of Home Affairs
Singapore

24. Tan Song Mong
Deputy Director
Security and Emergency Planning Office
Ministry of Education
Singapore

25. Denis Koh
Deputy Director
National Security Co-ordination Secretariat
Singapore

26. Mak Kum Wah (Col.)
Deputy Director
National Security Co-ordination Centre
Singapore

27. Patrick Nathan
Deputy Director
National Security Co-ordination Centre
Singapore

28. Joseph Lee Kim Leng
Deputy Director
Emergency Preparedness Division
Land Transport Authority
Singapore

29. Goh Yam Song
Deputy Director
Public Transport Security (Operations & Audits)
Division Land Transport Authority
Singapore

30. Chee Vui Chung
Deputy Director
National Resilience Division
Ministry of Information,
Communication and the Arts
Singapore

31. Steven Chiok Peng Meng
Deputy Manager
Public Transport Security (Operations & Audits)
Division Land Transport Authority
Singapore

32. Seow Kang Seng
Director
Consumer Safety & Crisis Management Department
Energy Market Authority
Singapore

33. Teong How Hwa
Director
Hazmat Department
Singapore Civil Defense Force

34. Chua Chong Kheng
Group Director
Rail Group
Land Transport Authority
Singapore

35. Dr K U Menon
Director
National Resilience Division
Ministry of Information,
Communication and the Arts
Singapore

36. Robin Tan Meng Heng
Director
Security & Emergency Planning Unit
Energy Market Authority
Singapore

37. Yeong Gah Hou
Director
National Security Co-ordination Secretariat
Singapore

38. Yeo Teck Guan
Director
Public Transport Security & Emergency
Preparedness Sub-group
Land Transport Authority
Singapore

39. Manimaran Pushpanatan
Deputy Commander
Special Operations Command
Singapore Police Force
Singapore

40. Chow Ngee Ken
Republic of Singapore Navy

41. Major Adrian Lee
Ministry of Defence
Singapore

LIST OF SPEAKERS / MODERATORS / PARTICIPANTS

42. Tee Eng Poh
Manager
Security & Emergency Planning Unit
Energy Market Authority
Singapore

43. Lee Liang Chye
Senior Assistant Director
3 Security Plans Branch (Emerging Threats/Technologies & Special Projects)
Ministry of Home Affairs
Singapore

44. Ong Choon Khiang Raymond
Senior Assistant Director
Strategic Development
Ministry of Home Affairs
Singapore

45. Lee Wai Hong
Senior Assistant Director
Emergency Preparedness
Ministry of Transport
Singapore

46. Gan Eng Khoon
Senior Assistant Director
Ministry of Transport
Singapore

47. Quek Siew Teck
Senior Deputy Director
Homefront Readiness and Evaluation Directorate
Ministry of Home Affairs
Singapore

48. Tham Jierong
Associate for MHA, Judiciary & AGC
Government Administration & Security Programmes
Ministry of Finance
Singapore

49. Chin Nyuk Khee Vivien
Planning Executive
Strategy Unit
Public Service Division

50. Lum Hock Meng
Head Bomb Data Centre
Singapore Police Force

51. Yolanda Chin
Associate Research Fellow
Centre of Excellence for National Security
S. Rajaratnam School of International Studies
Singapore

52. Hoo Tiang Boon
Associate Research Fellow
Centre of Excellence for National Security
S. Rajaratnam School of International Studies
Singapore

53. Ng Sue Chia
Associate Research Fellow
Centre of Excellence for National Security
S. Rajaratnam School of International Studies
Singapore

54. Nirupama Kishav
Research Analyst
Centre of Excellence for National Security
S. Rajaratnam School of International Studies
Singapore

ABOUT CENS

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

Why CENS?

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

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

What Research Does CENS Do?

CENS currently conducts research in three key areas of national security:

- Risk Assessment/Horizon Scanning
  - The art and science of detecting "weak signals" emanating from the total security environment so as to forewarn policymakers, the private sector and the public about approaching "shocks" such as terrorism, pandemics, energy crises and other easy-to-miss trends and ostensibly distant events.
- Social Resilience
  - The capacity of globalized, multicultural societies to hold together in the face of systemic shocks such as diseases and terrorist strikes.
- Homeland Defence Programme
  - The security of land-based, aviation and maritime transport networks and increasingly, the total supply chain vital to Singapore's economic vitality.
  - Health, water and food security.
  - Crisis communications and management.

How Does CENS Help Influence National Security Policy?

Through policy-oriented analytical commentaries and other research output directed at the national security policy community in Singapore and beyond, CENS staff members promote greater awareness of emerging threats as well as global best practices in responding to those threats. In addition, CENS organizes courses, seminars and workshops for local and foreign national security officials to facilitate networking and exposure to leading-edge thinking on the prevention of, and response to, national and homeland security threats.

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

To educate the wider public, CENS staff members regularly author articles in a number of security and intelligence related publications, as well as write op-ed analyses in leading newspapers.Radio and television interviews have allowed CENS staff to participate in and shape the public debate on critical issues such as risk assessment and horizon scanning, multiculturalism and social resilience, intelligence reform and defending critical infrastructure against mass-casualty terrorist attacks.

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

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

For More on CENS

Log on to http://www.rsis.edu.sg and follow the links to “Centre of Excellence for National Security”.

ABOUT RSIS

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

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

Graduate Training in International Affairs

RSIS offers an exacting graduate education in international affairs, taught by an international faculty of leading thinkers and practitioners. The teaching programme consists of the Master of Science (MSc) degrees in Strategic Studies, International Relations, International Political Economy, and Asian Studies as well as an MBA in International Studies taught jointly with the Nanyang Business School. The graduate teaching is distinguished by their focus on the Asia Pacific, the professional practice of international affairs, and the cultivation of academic depth. Over 150 students, the majority from abroad, are enrolled with the School. A small and select Ph.D. programme caters to advanced students whose interests match those of specific faculty members.

Research

RSIS research is conducted by five constituent Institutes and Centres: the Institute of Defence and Strategic Studies (IDSS, founded 1996), the International Centre for Political Violence and Terrorism Research (ICPVTR, 2002), the Centre of Excellence for National Security (CENS, 2006), the Consortium of Non-Traditional Security Studies in ASIA (NTS-Asia, 2007); and the Temasek Foundation Centre for Negotiations (2008). The focus of research is on issues relating to the security and stability of the Asia-Pacific region and their implications for Singapore and other countries in the region. The School has three professorships that bring distinguished scholars and practitioners to teach and to do research at the School. They are the S. Rajaratnam Professorship in Strategic Studies, the Ngee Ann Kongsi Professorship in International Relations, and the NTUC Professorship in International Economic Relations.

International Collaboration

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

ABOUT NSCS

The National Security Coordination Secretariat (NSCS) was set up in the Prime Minister's Office in Jul 2004 to facilitate national security policy coordination from a Whole-Of-Government perspective. NSCS reports to the Prime Minister through the Coordinating Minister for National Security (CMNS). The current CMNS is the Deputy Prime Minister Professor S. Jayakumar, who is also Minister for Law.

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

NSCS provides support to the ministerial-level Security Policy Review Committee (SPRC) and Senior official-level National Security Coordination Committee (NSCCom) and Intelligence Coordinating Committee (ICC). It 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.

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

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

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

Design by Oxygen Studio Designs