MINISTRY OF HOME AFFAIRS • 2010 ISSUE NO. 2

HOME TEAM JOURNAL

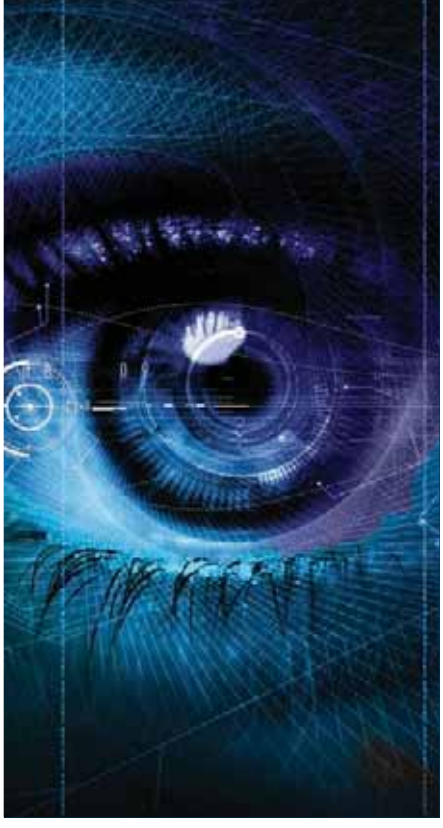
BY PRACTITIONERS, FOR PRACTITIONERS

INNOVATIONS IN HOMEFRONT SECURITY

HOME TEAM JOURNAL

ISSUE NO. 2

The Home Team Journal is a professional journal published by the Home Team Academy to highlight the work of the Home Team and its knowledge partners in Homefront Security and Safety. The Journal also functions as a forum for engagement, exchange and discussion over the broad and diverse range of issues and interests that come under the subject of Homefront security and safety.



EDITORIAL BOARD

Please address all contributions and correspondence to:

Editorial Board, Home Team Journal
Knowledge Management Branch, Strategic Affairs Centre
Home Team Academy
501 Old Choa Chu Kang Road, Singapore 698928

Email to MHA_HT_Journal@mha.gov.sg
Or fax to +65 6465-3793.

MINISTRY OF HOME AFFAIRS • 2010 ISSUE NO. 2

RESEARCH • INSIGHTS • TRAINING

FOREWORD

2 Foreword by Chairman

COVER STORY

4 Innovating to keep Innovating

14 Strategic Technology Planning in Home Team

FEATURE ARTICLES

26 How the Red Rhino was Born

31 The eVisitor Programme

43 APEC Trojan Email Attacks

47 Technology Crime Forensic Branch:
Hitting the Hard Drives

HOME TEAM PARTNERS

58 Thinking about the Future:
What the Public Service Can Do

67 Risk Assessment and Horizon Scanning Programmes:
The RAHS System

87 Bioterrorism in the Mail:
An Innovative USPIS Response to a New Challenge

94 Bioterrorism and the Role of Public Health

103 Suspect Detection System:
A Detective and Preventive Forensic Tool

HOME TEAM EXCHANGE

110 Homefront Insights: *Interview with Peter Ho*

121 New Media:
Potential Value for Home Team Agencies

135 Book Review: The Start-Up Nation
The Story of Israel's Economic Miracle

Foreword by Chairman

THE SECOND ISSUE of the Home Team Journal is in many ways continuing the journey we have embarked on; to create a repository of knowledge from the field of Homefront Security and Safety. In keeping with our tagline, '*for practitioners by practitioners'*, the second issue contains perspectives and initiatives by Home Team officers and our local and overseas partners on the topic, Innovations in Homefront Security (HFS).

I have to make an important caveat here. The articles from the Home Team that embody this theme don't simply talk about the latest gadget in the HFS field. Instead, they will also elaborate on how the idea of innovation has been reconstructed and manifested in the policies, programmes, and most importantly, is the people who must spearhead these initiatives. For many an innovative idea has met an early demise due to poor cultural buy-in and implementation. Thus, in many ways the idea is only the beginning. It starts with daring to think the impossible and challenging the conventional paradigm, if necessary and when faced with a unique problem. This is not simply 'a good to have' but something that in our present Homefront Security climate becomes an absolute necessity given the dynamic nature of our potential security threats and the pace in which they have evolved. We should not fail to meet the challenges of the future because of a failure of imagination.

We are honoured to feature an interview for the Home Team Journal on this theme with the former Head of the Singapore Civil Service, Permanent Secretary for the National Security and Intelligence Coordination (NSIC) and for Foreign Affairs, Mr. Peter Ho. This interview provides an overarching view on the changing landscape of Homefront Security in Singapore and his insights on how the Home Team can leverage on innovations and foster a culture of creativity.

We are once again grateful to have a very interesting mix of articles from our Home Team partners. Namely from our local Horizon Scanning Centre which is part of the National Security Co-ordination Secretariat, the US Postal Inspection Service, the US Centers for Disease Control and Prevention and

finally the Directorate of Forensic Sciences and Gujarat Forensic Sciences University in India.

I would also like to thank the encouraging comments, support and suggestions received from those who read our first issue. Please do keep the feedback and comments coming. We also welcome contributions from our Home Team officers and our local and international partners in Homefront Security.

Finally, I would like to thank the Editorial Team once again for keeping the idea behind the Home Team Journal alive. This is our innovation.

MR. DEREK PEREIRA
Chairman Editorial Board

Innovating to *keep* *Innovating*

MR. BENNY LIM, MR. JACKSON LIM, MR. TEONG HOW HWA

INNOVATION IS NOT NEW TO THE HOME TEAM

The Home Team departments have a long history of consistently enjoying a significantly high level of public confidence and trust. In the latest HDB Household Survey in 2008, the Police scored the highest amongst all other institutions for public trust and confidence.[1] In other surveys, public confidence in the Home Team to keep Singapore safe is consistently high.

No amount of creative public relations can account for this high level of public confidence. Ultimately, it is anchored to the Home Team's objective record of performance which has made Singapore one of the safest cities in the world.[2] This is a quality of life Singaporeans value, and one which expatriates living here value even more.

What is significant about this consistently good performance is the fact that it has been achieved in the face of significant and rapid changes in Singapore society and economy as well as in the region and beyond. This suggests that among other things, the Home Team departments and its officers have over many years been able to effectively adapt to and even exploit the opportunities of change to their operating realities, to stay on top of their game. This invariably entails innovation at work in these organisations.

Innovation therefore is not new to the Home Team in it's long history and experience even if the term "innovation" as a self-conscious label and buzz word in our public sector discourse, is of a younger vintage, dating to the early 80s. It is important to recognise this because it provides a critical historical context to any policy or plan to *promote innovation as a purposive and centrally managed programme* in the Home Team. This understanding of the organisation's history and its people is key to crafting the approach and engagement of any innovation programme in a manner best suited for it to connect, gain traction and succeed.

THE "INNOVATION" CAMPAIGN – WITS

HUMAN BEINGS ARE all capable of creativity and they innovate all the time. Whether this is expressed in our work or in our social relations or in other arenas, this innate potential, even if not of equal quality among us, resides in everyone. The aim of any organisation-wide innovation strategy should be to find effective ways to harvest the positive value that this creative potential in the individuals of its work-force have towards the achievement of its objectives or mission.

What was significant when the WITs (Work Improvement Team) movement began in the early 80s, was the bold recognition by the top leadership of the public service that the average worker has a useful perspective to offer to help find innovative solutions, precisely because he is in touch with the practical realities of the business often at the ground level – he has knowledge to offer from his direct experience; he knows of gaps, of persisting problems and contradictions and he has an appreciation of which solutions are more likely to work and which cannot. Hitherto, the tendency was to think of problem-solving in the organisation as the elevated province of managers and that the worker-bee's job was to just do and not ask why.

In the Home Team, the WITs movement in the first decade or so saw commitment at the highest level. Heads of Departments presided over their WITs programme and senior management made time to listen to presentations by the teams. As with all new enterprises, there were of course the skeptics but by and large, there was a significant degree of buy-in and positive spin-offs like team-bonding, acquiring new knowledge of analytical tools through WITs training and gaining exposure to new empowering experiences like presentations of ideas by the rank and file to their big bosses on how to improve a part of the business.

INNOVATION IN THE HOME TEAM – MORE THAN JUST WITS

IN THE HOME Team, our bottom-line is to keep Singapore safe and secure. Any useful idea that can help us better achieve our mission is welcomed. However an innovation is not just a promising idea.

Innovation in the organisational context is an idea that is operationalised to bring about a practical change to achieve either greater efficiency or effectiveness or both. This is the litmus test for innovation. Ideas which remain only as ideas are not innovations regardless how attractively imaginative or creative they are in their conceptions.

By this measure, the innovations in the Home Team – whether in terms of new products or change to process or business model – have been

considerable. The story of how the Red Rhino was born in the Singapore Civil Defence Force (SCDF) is an example of innovation at work.[3]

"Even more importantly, the leadership boldly reviewed and refined fire-fighting practice and assumptions which have been entrenched institutionally in the ogranisation for most part of its long history".

Fire engines are not built in Singapore and except for the choice of colours – typically yellow or red – we import fire engines ready-made. These are typically huge heavy vehicles carrying a crew of 6 to 8 men and packed with a large water tank as well as all kinds of heavy equipment and professional gear. In a congested city environment like Singapore, drivers of the fire engines face great difficulties negotiating narrow spaces and roads or lanes especially in the HDB heartland where 80% of its population live.

In 1998, the SCDF formed a project team to address this problem. The solution they came up with was launched in 2000 – a sleek, all-terrain fire-fighting vehicle which looked like a dune-buggy – it was much smaller, lighter and easier to manoeuvre than the standard fire engine. A public exercise was conducted, inviting the public to name the new vehicle – it was eventually called the "Red Rhino" and became the signature vehicle of the SCDF.

The Red Rhino story reflects a critical factor for successful innovation – *leadership support.* Officers working on the ground knew the operational challenge or problem. They were also critical to developing the solution and testing it. However to make the idea a practical innovation, there was need for leadership support to secure access to resources to develop the proto-type and pilot-test it.

Even more importantly, the leadership boldly reviewed and refined fire-fighting practice and assumptions which have been entrenched institutionally in the organisation for most part of its long history. The SCDF leadership saw the value of the Red Rhino, not as a replacement to the fire engine, but as a valuable complement to it – a fast response force able to handle incidents which do not require a fire engine. Even for those incidents which are larger and beyond the Red Rhino's capacity to manage, a forward professional force which can take early mitigating action and make a professional assessment on the ground of the nature and size of the threat, and what is needed to manage it, is invaluable to the operational planning of SCDF's incident management.

Analysis showed that most fire incidents attended to in Singapore could be managed effectively by the

Red Rhino. Use of its mist gun made for more efficient use of water and in turn, reduced the capacity of the water tank that needed to be borne on the vehicle (which was the largest part of the regular fire engine). And given Singapore's built-up urban terrain, water supply self-sufficiency was not critical since access to water was not a problem given the availability of risers which is a building requirement and a network of hydrants at road level. All this in turn meant that a smaller crew (4 men) and more limited equipage were sufficient to manage most of the fire incidents encountered. The speed of response – a dune buggy compared to a bus/ truck - also meant that the chances of putting out the fire early before it grows bigger are greater.

The story of the Red Rhino reflected not just innovation of product, but also of process and even the business model. The Red Rhino was also not a product of WITs. It was the result of the work of a project team, the members of which the SCDF leadership carefully selected, and tasked in a very targeted and focused manner. It was the result of a top-down or directed innovation. Indeed the resolve and commitment of the SCDF leadership to persist and drive the innovation to gain acceptance was crucial as there was initially strong resistance from the men, schooled as they had been, in a traditional fire fighting regimen which placed the fire engine as its staple resource in operations.

INNOVATION AND INNOVATION

Innovation in an organisation can be broadly described as purposively pursued at least at two levels. At one level, we have what has been called "incremental innovation" which involves mass participation typically via structured activities throughout the organisation. This is what our WITs movement is about and the innovation focus is usually about the efficiency of trying to do what we do better.

The second level is an older and more familiar form of top-down organisational structure for innovation. This level addresses what has been called "radical innovation" – typically requiring specialists whether housed in a permanent entity (e.g. strategic planning, science and technology development, strategic futures, scenario planning, horizon scanning outfits) or composed in the form of dedicated task-force or teams. Such outfits usually look at problems which are more complex and look for solutions which are strategic or for new knowledge or technology which are potentially game-changing.

Such specialist outfits also analyse trends and signals to anticipate the possible futures we may face – in the Home Team's case, these are changes

which have deep implications to the Home Team's prevailing ability to continue to achieve its mission in the future. Such changes if well analysed and understood, also typically offer critical opportunities for innovation.

"The overwhelming majority of successful innovations exploit change." "Systematic innovation therefore consists in the purposeful and organised search for changes, and in the systematic analysis of the opportunities such changes might offer for …innovation"[4].

LEADERSHIP – THE MOST VITAL FACTOR IN FOSTERING AN INNOVATION CULTURE

THE QUALITY OF leadership at all levels in an organisation is the single most important factor determining the depth and extent of success of the innovation strategy in any organisation. Above all, it sets the tone and values in the relationship between supervisor and the supervised which can either inhibit or facilitate innovation. Is staff feedback welcomed? Are staff members confident about surfacing ideas or reflecting problems and challenges that they see or face without risk of being misunderstood or embarrassed by being put down or rejected dismissively? Do we value the experience of our officers? Do we promote the habit of reflection over and learning from experience, especially by practitioners themselves?

The WITs movement created an officially endorsed discourse and a set of approved structures which provided a "safe" channel for staff to surface problems, to analyse them and offer solutions. It sought to empower each individual regardless of his status in the organisation to take ownership of the performance of his work unit and not just of himself. It sought to cultivate values and habits of practice which fostered a culture of innovation in the public sector. The hope was to develop in time, thinking officers imbued with the positive values of ownership and pride in their work and their organisation.

The value of the innovation programme in the Home Team is not just to discover the specific innovation itself that would promote greater efficiency or solve a problem at work. It is even more important to promote the broader development of an innovation culture. This is more valuable than any single innovation. This is because invariably, such a culture means having developed adaptive and thinking officers who are engaged.

This is more critical today then ever before. An organisation of such officers will be better placed to possess and exercise the adaptive reflexes and capacities to survive disruptive operating and

environmental change, and to be able to overcome the surprises and critical challenges in their work that these will entail.

Creating and rooting practices to develop such a culture of innovation, adaptability and receptiveness to change in the public service was a key value in WITs. This was perhaps the reason why mass participation became such a fixation in the central management of the WITs movement. While the first 10 years of the WITs movement probably held more gains than losses, the decades that followed (until interventions in recent years) provoked widespread cynicism. Participation became a chore and for many managers including those in the Home Team, the WITs movement became a numbers game.

The story of the WITs movement is a subject that merits deeper research and a full case history. However, in the Home Team, what was clear was that meeting KPIs (Key Performannce Indicators) imposed centrally became an end in themselves and led to a distortion of intended behaviour. Form displaced substance; quantity replaced quality.[5] The innovation movement in the Home Team, as elsewhere, became undermined by bureaucractic excesses and rigidities in the management of the programme itself, ironically the very thing – stifling barriers to innovation – that the movement and its programme were conceived to remove.

REVITALISING THE INNOVATION MOVEMENT IN THE HOME TEAM

ONE SIZE DOES not fit all and certainly not over time. Progress in the innovation journey among different people in different organisations is inevitably uneven. Hence, more and more departments and their staff outgrew the WITs analytical tool-kit and its rigid forms of presentation. Indeed, after the first harvest of low hanging fruits, the next order of meaningful problems tackled are usually more demanding. They also require more extended time-lines than adherence to the annual calendar that the WITs cycle allowed.

Fortunately, these excesses and rigidities are recognised and being addressed. The focus is more outcome-based. We have liberalised the forms of innovation activity and hopefully lower the barriers to participation. In the Home Team, departments are today free to adopt and implement initiatives as well as to seek out, create and exploit opportunities based on the specific realities of their organisation and operating terrain.

The Home Team (HT) Departments have in recent years created their own forms of engagement. The SCDF launched its Innoventure Club in July 2009 for its officers from various units with a keen interest in innovation-

related activities. The Singapore Police Force (SPF) has decided to form Innovation Teams across their Land Divisions and Specialist Units with a special writ to challenge deep-seated assumptions as well as established protocol and procedures. This focus recognises the concern of officers on the ground becoming SOP (Standard Operating Procedure) compliant but less effective when scenarios are different from those prescribed in the SOP.

With the lifting of prescribed quotas or numbers for teams, we have not surprisingly seen a significant reduction in the number of WITs – from 2133 teams in 2008 to 1488 teams in 2009. Although the number of teams has been reduced, what is significant is that the total efficiency cost savings from WITs projects saw an increase from $1 million in 2008 to $8 million in 2009. This, in our assessment, is a sign of quality and meaningful participation returning to the Home Team innovation programme.[6]

In 2009, the organisers of the annual Ministry of Home Affairs (MHA) 3i Convention (traditionally, a platform to showcase new products and innovations developed by Home Team officers) sought to refresh the event by combining it with an entirely new programme viz SAFE (Security Awareness for Everyone) programme. The SAFE programme is an experiment where MHA provides a platform to engage youths and students to generate innovations in the field of safety and security. The new event was called the MHA Innovation Festival. Held on 2 Oct 2009, it drew 1500 participants and visitors, consisting of HT officers, students and representatives from other ministries.

Besides adding much energy and buzz to the event, such participation by youths allowed the mixing of ideas between HT officers and the students. It also provided an effective platform to engage youths - a key constituency for the Home Team in its work. One tangible outcome was the opportunity for many of these raw ideas by the students to be further fine-tuned with the help of Home Team mentors and developed into practical solutions.[7]

The MHA Core Innovation Fund was set up in 2008 to provide funding to support those who have an innovation proposal. This resource gives the Home Team innovation managers the means to support experimentation. However, the teams or officers have to compete for funding and an inter-agency Innovation Evaluation Working Group (IEWG) will jointly evaluate their proposals. Such a working group, in turn, provides a practical platform to facilitate the sharing of experiences and the cross fertilisation of ideas across the HT Departments.

An Innovation Database is in the pipeline to serve as a central repository for all past successes and

failed attempts of innovation. This provides opportunities for learning and networking with like-minded adopters of innovations. It allows us to re-visit good ideas which for one reason or another could not be operationalised. For instance, the idea of the Fire Fighting Grenade which SCDF tested previously and found operationally effective but not cost effective, can be revisited periodically to see if and when new technology or changes in production pricing makes the idea viable.

The Staff Suggestion Scheme – an old and low cost form of mass participation in the innovation programme – has continued to attract high staff participation. In 2009, more than 87,000 suggestions were received; higher than the nearly 77,000 received the year before. This is an engagement instrument which has good potential for qualitative improvement. It clearly enjoys a degree of natural traction with Home Team staff and has a potential application value for crowd-sourcing. There is merit to see how we can innovate the humble Staff Suggestion Scheme.

INNOVATION – CONTROL AND THE DYNAMICS OF BALANCE

INNOVATION IN ANY organisation, the Home Team included, cannot be a free-for-all pursuit backed by limitless resources. It has to be purposive and invariably related to achieving the mission and objectives of the organisation. Structures to manage and direct the development of innovation efforts as well as the cultivation of the values and habits of innovation as part of organisational culture are as unavoidable as they are necessary.

The question is really about the right balance. What is the optimal form for management structures that facilitates rather than stifles or inhibits innovation? For one thing, innovation should not be restricted to be achievable only via one form; it should not for instance, be WITs-bound. Diversity is a valuable dimension of the Home Team organisation. The challenge for management should be how to exploit the positive value in this diversity as well as encourage collaboration and sharing across it.

"Structures to manage and direct the development of innovation efforts as well as the cultivation of the values and habits of innovation as part of organisational culture are as unavoidable as they are necessary"

The Home Team experience has been one where the old adage of necessity being the mother of invention has proven true. The many successful e-services which

the Immigration & Checkpoints Authority (ICA) have innovatively developed were driven in part at least by the fact that many of these arose from necessity as officers faced a severe manpower crunch with no prospect of relief.[8] But what is the optimum level of pressure or tension that spurs staff to innovate rather than deflates enthusiasm, defeats and demoralises them?

Knowing the right balance of control and freedom, direction and free-play requires the exercise of judgement. Understanding the dynamics of history and people at work and the prevailing culture of the organisation helps make that judgement more informed. For instance, knowing how to articulate the new idea or innovation in terms familiar to the target user group or knowing who the key players among them you should convince and convert as early adopters to drive diffusion of the innovation, is important to success.[9]

Knowing the practical ground realities of the organisation and securing honest feedback from its people are critical in innovation. "Innovation is both conceptual and perceptual. The imperative of innovation is therefore to go out and look, to ask, to listen."[10] This applies no less to the manager who is responsible for the innovation programme in his organisation because he is also an innovator.

The manager who oversees the innovation programme in the Home Team departments must realise that he is not exempt from the very processes he is promoting. In crafting his strategy and interventions to promote innovation, he needs to reach out, engage and listen to his intended audience, then make adjustments to the approaches conceived and watch closely how it takes root or otherwise when operationalised. He needs to be adaptive and innovative in the application of his programme and the formulation of strategies to keep in tandem with the changes that occur within his organisation and how staff relate to the different aspects of the programme. In short, he also needs to innovate to keep innovation healthy and alive.

ENDNOTES

[1] In the HDB Household Survey 2008, the Police scored the highest among respondents for public confidence at 7.6 followed closely by the judiciary (7.5) and religious institutions (7.4).

[2] Crime rate in Singapore for 2009 is 661 per 100,000 population, lower than other cities like Hong Kong, London, New York, Tokyo and Sydney. The PERC Report 2007 showed Singapore as having the lowest number of crime threats against persons and property. The World Fire Statistics 2007 rated Singapore among the most fire safe countries in the world. The UN Office on Drugs and Crime stated in its World Drug Report 2008 that Singapore has the lowest annual prevalence for abuse of opiates, amphetamines, cannabis and ecstasy.

[3] See article in this issue of the Home Team Journal titled "How the Red Rhino was Born" by Teong How Hwa.

[4] Peter Drucker (1985) "Innovation & Entreprene urship"(Butterworth-Heinemann – re-printed 2007)

[5] It became so prescriptive that in WITs competition, any other analytical tool in place of the Fish-Bone chart would score no points regardless if the analytical approach used was more suited to address the problem in question.

[6] One issue that needs to be addressed is the question whether or not, the kinds of problems and challenges in the Home Team today are more sophisticated and demand resources beyond a single WIT. There is merit in exploring whether or not an innovation approach which relies on multiple WITs coordinated as a group or cluster is a suitable option. Additionally, a common refrain heard these days from many WITs members is that they have run out of topics or issues at their work unit level to tackle as all the low hanging fruits have been harvested. Perhaps soliciting suggestions from across the organisation as well as posing problem issues by management and then inviting WITs to choose which to adopt and pursue can be a means of refreshing the well of ideas and reversing the dry-spell.

[7] One such idea is the development of an anti-snatch theft device by a group of ITE students. The requirements are made based on actual feedback from senior citizens interviewed. This device now has three iterations and also sparked interests for commercial production.

[8] The range of ICA transactions which can be conducted on-line now includes booking, changing or canceling appointment for services with ICA, application for NRIC, renewal or transfer of re-entry permits, extension of short-term social visit pass application, visa and extension of stay, registration of student pass.

[9] "For rapid diffusion of ideas to occur, nothing beats compatibility." Receptivity is enhanced when the new idea is articulated in a manner "compatible with existing frameworks of thought" in the organisation. Gregory Berns (2010) – " Iconoclast" (Harvard Business Press) pp184-189

[10] Peter Drucker (1985) "Innovation and Entrepreneurship" (Butterworth Heinemann 2007) p44 and p123

EDITOR'S NOTES

Our cover story shares insights and lessons about managing innovation in the Home Team which is learnt from its experience in the public sector's innovation journey. This cover story is jointly written by Mr Benny Lim, Permanent Secretary, Ministry of Home Affairs (MHA), Mr Jackson Lim, Senior Director, Strategic Planning and Development Division (SPD), MHA and Mr Teong How Hwa, Deputy Director, SPD, MHA.

Strategic Technology Planning *in the* Home Team

MR. CHEN TZE PENN, MS. TEO MUN ENG

TECHNOLOGY IS STRONGLY associated with the idea of innovation. This is not surprising given the dizzying speed of technological advancement in the last few decades and the pervasive impact of technology on our lives, for good and for bad.

Terrorists today have access to many of the latest technologies and have exploited them to inflict the maximum damage possible. To stay ahead of our adversaries, especially when faced with tight resource constraints such as manpower, the Home Team must leverage on technological innovation as a key strategy to raise productivity and enhance Singapore's security posture.

We must constantly adapt to the fast-changing technological landscape and ensure close 'business-to-technology' alignments. This requires a strong leadership to build an adaptive and innovative culture that can respond rapidly to changing external conditions. It also requires a well-managed organisational process with specific tools, rules and discipline to generate, evaluate and experiment with new ideas. Generating fresh ideas, identifying new opportunities, exploiting new technologies are not solely managerial tasks, but are also organisation-wide tasks.

To leverage on technological innovation, the Technology and Infrastructure (T&I) Division has developed and implemented a Strategic Technology Planning (STP) framework. It is a formal process that brings together relevant Operational and Technology Officers from Ministry Headquarters (HQ) and the Home Team Departments (HTDs) to address the entire technology value chain from identification, to tracking, to evaluation and adoption. Through close ops-tech collaboration, Strategic Technology Planning helps to ensure that the Home Team adopts new technologies that can meet its challenges effectively and efficiently.

The specific objectives of Strategic Technology Planning are as follows:

i. Minimise the duplication of efforts, resources and funds
ii. Facilitate joint evaluation of technology by the Home Team
iii. Build up technological expertise within the Home Team, and
iv. Help officers in the Home Team harness technologies applicable to their operational environments.

The Ministry's Enterprise Architecture Governance Council is the Steering Committee that drives and provides direction to MHA Strategic Technology Planning. It is chaired by Deputy Secretary/ Security and comprises the Deputy Heads of Departments and the Senior Directors of the Technology & Infrastructure, Strategic Planning and Homefront Security Divisions.

The Strategic Technology Core Team (STCT) was formed to support the Steering Committee. It comprises officers from the Information Technology Branch (ITB) and Technology Development Branch (TDB) in T&I Division, and IT representatives from HTDs. Its primary focus is on technologies with potential impact across the Home Team while at the same time maintaining oversight of technology trials that are undertaken by the respective HTDs to serve their specific needs.

STRATEGIC TECHNOLOGY PLANNING PROCESS

The Strategic Technology Planning process consists of five stages, namely, Scope, Track, Prioritise, Evaluate and Encourage Adoption[1]. The five-stage formalised process is used to find promising candidates from the vast and ever-changing array of technologies available for consideration for deployment by the Home Team. The diagram (Fig 1) below depicts the iterative nature of the process.

Fig 1: Five-Stage Process of the Strategic Technology Planning

Stage 1: Scope

The main purpose of this stage is to provide focus for Strategic Technology Planning by identifying technologies which are aligned to business objectives. In this stage, the STCT also helps the HTDs understand how emerging technologies can and will shape their business models, operations and processes. To ensure alignment to the Home Team's broad strategic directions, and to meet the respective

HTDs' operational needs, the STCT uses the following key inputs to this stage of the planning process:

i. MHA Strategic Planning Guidance
ii. MHA Enterprise Architecture
iii. Technology needs identified by HTDs (Technology Watchlists) and emerging technologies (i.e. immature or mature but have yet to achieve their potential level of acceptance and adoption) which might be useful to Home Team.

The diagram below (Fig 2) depicts how the above inputs are simultaneously used to facilitate Stage 1 of the Strategic Planning Process.

Fig 2: Inputs to Stage 1 of the Strategic Technology Planning Process

The outcome from Stage 1 is a list of technologies identified to be of operational importance to HTDs. These technologies will be further categorised for the respective Technology Clusters to conduct a more focused evaluation for possible Home Team adoption.

As part of the effort to identify new technologies of interest to the Home Team, the STCT forms new Technology Clusters and also reviews existing ones to ensure their relevance to the changing business needs of the Home Team.

One of the biggest challenges in this stage is the daunting task of sieving through reports by the various vendors claiming superiority for their technology products. Differing product positioning and levels of technology complexity can inhibit comparisons of vendor offerings. In addition, the development paths of emerging technologies are often unclear because of their immaturity. The STCT relies heavily on information provided by IT research and advisory services' vendors to reduce the amount of time spent in assessing technology products.

TECHNOLOGY CLUSTERS IN STRATEGIC TECHNOLOGY PLANNING

TECHNOLOGY CLUSTERS ARE formed to carry out the remaining stages of the Strategic Technology Planning process. Every Technology Cluster plays a crucial role in ensuring the successful execution of Strategic Technology Planning in the Home Team. Over the last two years, five Technology Clusters have been formed. They are:

i. **Video Analytics** – covers technologies associated with the analysis of video images in order to detect individuals behaving in specific ways (e.g. loitering, fighting) or vehicles of interest. This Technology Cluster also looks at technologies that aid in image processing as well as video capturing and transmission.

ii. **Tracking** – covers technologies associated with the tracking of persons and assets, as well as location-related applications. The technologies under this Technology Cluster are grouped under 3 categories, namely island-wide tracking, localised tracking and routing & location-based applications.

iii. **Business Analytics** – covers technologies associated with the continuous iterative exploration and investigation of past business data to gain insights, guide planning and make decisions through statistical and quantitative analysis.

iv. **Communications** – covers wireless communications technologies needed to facilitate effective voice and data communications for HTDs.

v. **Modeling, Training and Simulation** – covers technologies related to the exploration of modeling, training and simulation. Here, we look at different types of systems which can range from advanced systems that have integrated live and virtual environments to task level simulation systems.

Each Technology Cluster comprises one STCT member, technology representatives from the HTDs' Technology Divisions and operational representatives (i.e. end-user representatives). The HTD operational representatives are responsible to provide the business requirements and to facilitate the sharing of trial findings and technology adoption in their HTDs.

Stages 2 to 5 of the Strategic Technology Planning are carried out by the Technology Clusters in the following manner:

Stage 2: Track

TECHNOLOGY TRACKING INVOLVES scanning and watching for new technology developments within each Technology Cluster, and capturing information about the associated emerging technologies in a format that facilitates subsequent prioritisation and evaluation. For each technology identified, the Technology

Cluster develops a technology profile comprising the following attributes:

1. Name and definition of technology
2. Business applications
3. Benefit to MHA
4. Potential business champion, and
5. Home Team Departments interested/investigating this technology
6. Leading vendors
7. Costs

The technology profiles serve as inputs for the subsequent stages of Strategic Technology Planning as well as a source of valuable information about a specific technology for the Home Team.

Stage 3: Prioritise

The objective of prioritisation is to select a subset of the emerging technologies within the Technology Cluster that look the most promising to the Home Team. If the Technology Cluster were to find the number of technologies identified under Stage 2 manageable, they can decide to skip this stage and proceed to the next stage. The following are possible criteria to rank the list of technologies identified:

1. Level of Maturity
2. Level of Disruption
3. Benefit to the Home Team

1. Level of Maturity (High, Moderate, or Low)

a. High
The established business case in using the technology is clear and there are numerous examples of mass adoption of the technology.

b. Moderate
There are some clearly defined applications for the technology where the benefits far outweigh the problems encountered with the technology.

c. Low
The technology is most likely applied in demonstrations, prototypes and pilots with few deployed applications.

Technologies that score high on the level of maturity will be of immediate interest to the Technology Clusters for them to evaluate the potential areas of application in the Home Team.

2. Level of Disruption (High, Moderate, Low)

a. High
As an example, this could mean that a complete replacement of network, hardware, and software or business infrastructure is needed in order to introduce the technology.

b. Moderate
Adoption of the technology only requires replacement of some elements of the infrastructure.

c. Low
Adoption of the technology requires only minor modifications or additions of specific applications, workstations, peripherals or processes to be made.

3. Benefit to the Home Team

a. Transformational
The technology enables totally new ways of operating the Home Team's business. This results in significant improvement in the Home Team's key performance indicators (KPIs).

b. High
The technology enables some new ways of performing specific operational areas in Home Team resulting in improvement in the Home Team's KPIs.

c. Moderate
The technology provides incremental improvements to established processes in the Home Team resulting in some improvements in the Home Team's KPIs.

d. **Low**
The technology provides little or no improvement to established processes in the Home Team and hence will not result in any improvement to the Home Team's KPIs.

The greatest benefits that can be harnessed are those that are transformational in nature. Therefore it is of utmost importance to put resources into technologies that can potentially transform the way the Home Team carries out its business.

The outcome of this Stage is the selection of a subset of the emerging technologies within each Technology Cluster for detailed evaluation. The Technology Cluster will seek the necessary funding to evaluate these selected technologies. Various sources of funding are available, one of which is the Ministry's Core Innovation Fund.

Stage 4: Evaluate

THE PURPOSE OF this stage is to investigate the list of prioritised emerging technologies in order to attain sufficient knowledge about the technology and to determine whether the technology is suitable for adoption.

Depending on the availability of resources, the Technology Cluster can decide on whether to kick-start evaluation on all prioritised technologies or start with only the higher priority technologies. An evaluation project team under the

Technology Cluster will be formed for each technology to be evaluated. The project team comprises of both operations and technology officers. This enables operational users' inputs to be immediately taken into consideration at the technology evaluation stage. From experience, the rate of success from a technology trial leading to an effective deployment increases significantly with the formation of project teams that emphasises ops-tech collaboration.

> Depending on the needs and circumstances, there are several approaches to conducting the evaluation and these can include paper investigations, trials, prototyping and pilots.

The key deliverable from an evaluation activity is a decision as to whether or not to proceed with a specific adoption of the technology. At the end of the evaluation, the team may recommend one of the following outcomes:

i. Proceed to operational deployment;
ii. Revisit the evaluation in a revised form (for example, with a different application or alternative product);
iii. Return the technology to the tracking stage until it matures further; or
iv. Remove the technology from the portfolio of technologies that are being tracked.

A decision not to proceed with the deployment of a technology should not be viewed as a failure. It can save the Home Team considerable downstream expenses and unnecessary challenges (e.g. integration problems or disruptions to existing infrastructure) by establishing key facts about a technology early rather than after the procurement process is initiated.

For technologies that are found suitable for adoption, the next stage is to encourage their use in the Home Team.

Stage 5: Encourage Adoption

THE ACTIVITIES ASSOCIATED with encouraging the use of technologies can include:

a. Education and Promotion
This involves creating awareness of the technology in the Home Team, what value it brings to the Home Team and the application opportunities.

b. Facilitate Procurement/ Implementation
This involves defining the typical requirements and standards for using the technology. Standards will be established in the Technical Architecture under the MHA Enterprise

Architecture to facilitate system interoperability and faster deployment of new technologies as HTDs do not need to grapple with varying emerging standards.

c. Removing Obstacles to Adoption

This involves examining if there are any obstacles, such as operational or technical challenges that can hinder adoption and to identify solutions to overcome them.

BENEFITS OF STRATEGIC TECHNOLOGY PLANNING

Having a Strategic Technology Planning process in the Home Team has smoothened the way for the identification and implementation of emerging technologies that are useful for the Home Team. Specifically, Strategic Technology Planning has brought about the following for the Home Team:

a. Closer collaboration

Co-ordinating technology scanning activities across the HTDs has minimised the duplication of efforts and enabled HTDs to leverage and build on the successes of each other. This process also allows decisions about the technologies to be made based on an alignment with the Home Team strategies and goals while ensuring that individual HTDs' business needs are met.

b. Information Sharing

Information gathered is shared through the Technology Clusters and STCT and in this way is made available to all HTDs. In April 2010, T&I has launched a Strategic Technology Planning Website to further facilitate the sharing of information so that the HTDs can easily keep abreast of the types of emerging technologies which are being evaluated and the kind of evaluation which have been or will be conducted in the Home Team. The features of the website include tools to manage the technology exploration of HTDs and Technology Clusters, as well as to share technology watchlists and evaluation reports. The features are depicted in the diagram (Fig 3) on the next page.

c. Cost Savings

With a common front to engage the technology vendors, the Home Team is also able to avoid duplication of efforts in evaluating a new technology. This will result in cost savings.

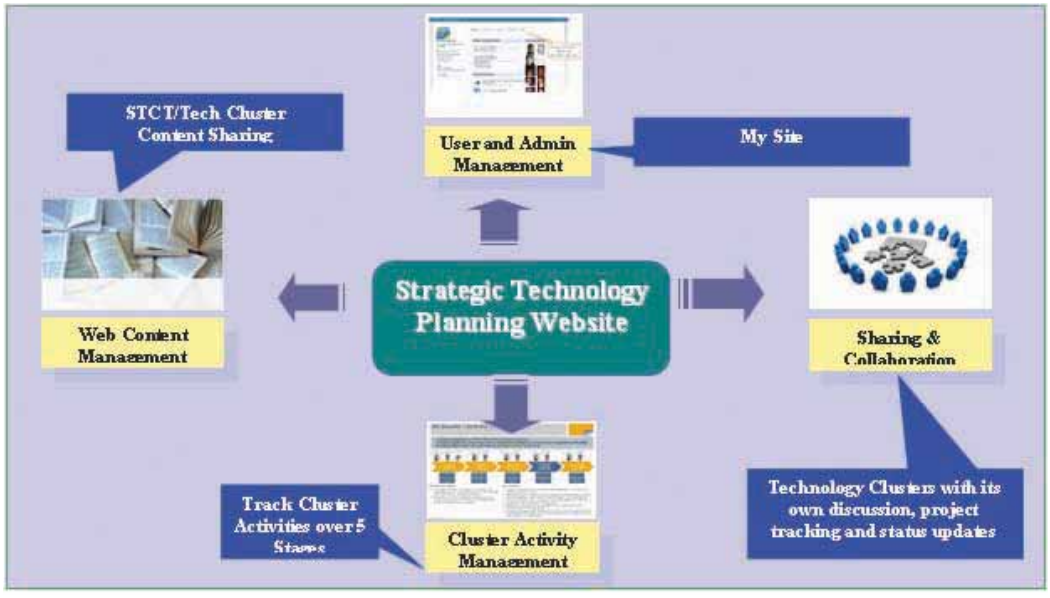


Fig 3: Strategic Technology Planning website

TECHNOLOGY CLUSTER TRIALS

MANY TECHNOLOGY TRIALS have been carried out by the Technology Clusters. Here are some highlights:

Fig 4: Sample Business Analytics dashboard

a. Business Analytics Technology Cluster

i. **Central Narcotics Bureau (CNB) Trial on Drug Offences.** This trial looked at combining various CNB data sources, namely databases, excel files and access databases, to get a holistic view of drug offences' trends and statistics. The trial has proven that the deployment of the business analytics tool can result in cost savings as data/information can be readily available at the analysts' fingertips without the need for time-consuming report generation. In addition, the tools can enable the portability of information as the dashboard can be viewed offline on a standalone notebook.

The trial also showcased the ability for analysts to uncover possible reasons behind the drug offence trends in the shortest possible time. For example, analysts are able to

drill into the data to identify reasons for significant spikes in offence trend for a particular drug type (e.g. detecting increased offences from a particular race and age group).

In summary, the CNB trial has been successful in highlighting the benefits of the business analytics software, such as dashboard and statistical analysis, to the CNB's users.

ii. Ministry HQ's trial on the effectiveness of corporal punishment using Prisons Services' (SPS) operational data.

This trial employed more advanced data mining capabilities to analyse, compare and study cohorts of ex-offenders who were imposed with and without judicial punishments.

The trial was able to show the basic trends of offender behaviour as well as the forecast of the trends.

The analysts employed correlation analysis on the available data, for example, to identify the most likely factors contributing to repeat offender behaviour. Such information will be helpful to assist MHA in policy making. In addition, the predictive modelling capability enabled analysts to identify "high risk" offenders who were more likely to repeat their offences.

Together with other data mining capabilities, such as pattern discovery, the trial has proven that the data mining tools can enhance the depth of researchers' analysis on available data. The research results can in turn be used to aid policy making and strategic decision making.

Fig 5: Sample Business Analytics dashboard to show trend and forecasts

b. Video Analytics Technology Cluster

i. Mobile Automatic Vehicle Screening System Trial.

This trial evaluated the effectiveness of mobile Automatic Number Plate Recognition (ANPR) systems. The limitations of such mobile ANPR systems and the effects of environmental lighting and weather on ANPR accuracy were studied. Several systems were tested and these included interior and exterior mounted ANPR camera systems (see pictures below).

The mobile ANPR system will enable our frontline officers to rapidly screen vehicles passing by the Home Team's fast response cars and alert officers to any vehicles of interest detected. The trial was successfully completed, and SPF is currently evaluating the approach to implementing the technology.

ii. Video Content Search (VCS) Trial.

This trial aimed to determine if currently available VCS software can be applied to video footage taken from existing close circuit television cameras used for general surveillance. The VCS software was tested for its ability to search through video footage for objects based on the object's colour (e.g. a red car or a person wearing blue).

The VCS software enables investigation officers to search through large volumes of archived video footage to find an item or person of interest. This will help to narrow down their search and reduce search times. The trial has provided insights into the capability of the software in using existing CCTV footages.

c. Modeling, Training and Simulation Technology Cluster

The Technology Cluster is working closely with the Singapore Civil

Fig 6: External pan-tilt-zoom camera

Fig 7: Internally mounted fixed camera

Defence Force (SCDF) to explore an integrated live and virtual environment training and simulation system. This kind of training and simulation system will allow the HTDs to train in realistic environments which are costly or impossible to create in real life environments. The frequency of training can also be increased and the actions of all participants can be recorded for post-training reviews, thus raising the capabilities and proficiencies of our Home Team officers.

Fig 8: VCS Software on CCTV Footage

CONCLUSION

Through the Strategic Technology Planning process, the Home Team can operationalise its key strategy for leveraging on technological innovation to meet the daunting challenges of Homeland Security. In addition, Strategic Technology Planning provides a systematic way of identifying technologies that can act as force multipliers for the Home Team. It takes into account operational needs and marries these with emerging technological capabilities to help MHA achieve its mission of a safe and secure home.

REFERENCES

1. Five Stage Strategic Technology Planning Process is adapted from Gartner Research article - 'STREET Framework Applies to Distributed Innovation', by Jackie Fenn, May 2007.

EDITOR'S NOTES

Mr. Chen Tze Penn is the Senior Director, of the Technology & Infrastructure Division of MHQ/ MHA. Ms. Teo Mun Eng is the Director of the Information Technology Branch, T& I Division.

The Technology and Infrastructure (T&I) Division works in close consultation and coordination with all the departments in MHA to ensure that their operations are well supported by up to date and cost-effective technologies. It plays a critical role in supporting innovation through technology.

How the *Red Rhino* was Born

MR. TEONG HOW HWA

THE CONVENTIONAL FIRE engine is indispensable for handling major incidents such as larger-scale industrial and commercial fires. However, the development of modern high-rise residential and industrial buildings and estates in Singapore gave rise to entry and access limitations. Examples include multi-storey car parks, sheltered pedestrian walkways and narrow vehicular access routes.

This in turn placed severe limitations on the conventional pumpers. Their large chassis and frame make it relatively difficult for them to gain entry using narrow, low or restricted access routes. The fire pumpers also encountered difficulties going off the road in order to attack fires at close range.

INNOVATION – FROM IDEA TO PRODUCT

SCDF MANAGEMENT DIRECTED a study of the problem and significance. Over the years, there was a generally well developed fire safety culture in industry and fire safety building requirements and standards were comprehensively and clearly articulated and complied with. A robust inspection regime by SCDF gave it confidence as well that this state of affairs would be sustained. As such, major fires in industry and commercial establishments in Singapore were exceptional and not a frequent occurrence.

Analysis of fire statistics of incidents showed instead that most fires were in small, high-rise residential apartments in the public housing heartland. Indeed there was a trend of consistent increase in the occurrence of such fires. With comprehensive fire safety provisions in high-rise buildings (i.e. water risers in place) and a reliable hydrant network available in Singapore, the need for a fire engine to carry self-sufficient water supply was less critical in such incidents. This in turn raised the practical possibility of a smaller operational vehicle with a leaner fire fighting crew.

This was not a new direction in the development of operational capabilities. Fire bikes had been

introduced to allow for a speedy response time than the regular fire pumpers/engines. However fire bikes had obvious limitations in terms of what it can carry in equipage and fire fighting capacities. Even if water is tapped from an external source at the incident site itself, bikes could not carry hoses or pressure pumps.

A mid-size solution appears the pragmatic direction to pursue – a highly mobile and speedier fire appliance that can complement the existing capabilities of the fire bikes and that of the conventional fire pumpers/engines. The SCDF leadership established a project team composed of selected officers and tasked it to look into the possibility of having a custom-built all-terrain vehicle with an aim to enhance our fire-fighting capabilities in combating fires within housing estates in urban settings.

The project team worked with industry players and developed the concept and operational and technical requirements of a proto-type vehicle. The SCDF team also worked out the specific list of items that the vehicle is required to carry based on the kind of scenarios it was likely to be deployed in.

In 1999, the available options of the chassis of what was essentially a vehicle heavier than standard vehicles of the same size in the market, were analysed for the prototype and the design and layout was determined. Field testing was conducted and all further modifications were completed in Mar 2000.

In Apr 2000, the prototypes were deployed at Bt Timah and Ang Mo Kio Fire Stations, which have a high proportion of residential houses, to assess the performance of the prototype for a period of 1 year. Additionally, the SCDF management assess that these stations had commanders who were willing to try out the proto-type and to mobilise their men behind it. The trial was a success as the appliance was able to manoeuvre within confined spaces, mount curb and accelerate on steep ground.

CAPABILITIES OF THE RED RHINO VIS-À-VIS THE STANDARD FIRE ENGINE/PUMPER

The Red Rhino is much smaller in size in comparison with the traditional fire engine. In terms of operational performance, the Red Rhino's water pumping capacity and flow rate is also lower than what is performed by the fire engine. However, the capabilities provided by the Red Rhino are suffice to tackle most of the small fires and simpler rescue incidents.

IMPACT OF THE RED RHINO

With the Red Rhinos, a valuable operational option was made available to SCDF to match response with the threat. Fire pumpers could be

	Traditional Fire engine/ Pumper	Red Rhino (1st generation)	Red Rhino (2nd generation)
Water tank size	3600 litres	50 litres	50 litres
Pump capacity (up to)	4546 litres per minute	2000 litres per minute	2000 litres per minute
Chassis Size	8.7m x 2.5m x 3.4m	5.5m x 2.0m x 2.0m	5.1m x 1.9m x 1.9m Red Rhino 2.0 is 10% smaller and 40% lighter than the 1st generation. This was made possible with the introduction of a smaller and lighter water pump which is able to deliver the same performance.
Main features	• Full range of rescue equipment including those for height rescue like ladders • Fixed water monitor head	• 4x4 vehicular capability • Selected rescue equipment including forcible entry tools, hydraulic cutter and spreader • The ability to maintain pumping operations while the vehicle is mobile • Detachable water monitor head	• 4x4 vehicular capability • Selected rescue equipment including forcible entry tools, hydraulic cutter and spreader • The ability to maintain pumping operations while the vehicle is mobile • Detachable water monitor head • Red Rhino 2.0 is designed to enhance safety with features like roll over cages, ABS (Anti-Lock Braking System), EBD (electronic brake force distribution) and better optimised centre of gravity

activated for larger scale fires while the fire bikes and Red Rhinos could be sent for smaller fires. Alternatively a combination of resources could also be dispatched to deal with incidents. To date all the fire stations, with the exception of Jurong Island and Banyan FS, are equipped with Red Rhinos.

Based on the statistics over the last few years, the Red Rhinos has proven to be highly effective in tackling small to medium size fires and simple rescue incidents. About 40% of the annual fire calls and rescue incidents are handled by the Red Rhinos.

Year	Total No of Fire Incidents	Fire Incident attended by Red Rhino	Total No of Rescue Incidents	Rescue Incident attended by Red Rhino
2007	4796	2850 (59.4%)	1639	1041 (63.5%)
2008	4973	2408 (48.4%)	2371	850 (35.8%)
2009	5235	2345 (44.8%)	2508	938 (37.4%)

A positive spin-off arose when the Red Rhino became available. The Red Rhino proved instrumental to the creation of a new forward deployment arrangement – the establishment of Satellite Fire Posts (SFPs). Response times depended much on travel speed from fire station to incident site. The increasing volume of traffic over time in Singapore roads made this more challenging. SFPs helped mitigate this problem and became strategically located extensions to conventional Fire Stations in order to reduce response timings.

The SFPs are located at the void decks of Housing & Development Board (HDB) blocks and the cost of establishing a SFP is just 10% that of a conventional Fire Station. Due to its compact size and low weight, the Red Rhino can be parked at any normal parking lot without inconveniencing the other HDB vehicle owner-residents.

FURTHER ENHANCEMENTS – RED RHINO 2.0

In 2009, the Red Rhino underwent design and construction enhancement. The newly designed Red Rhino, is aimed to enhance the vehicle's accessibility to even tighter and narrower spaces while improving vehicle safety and environment efficiency. The end result is a product which is 10% smaller and 40% lighter than the original version. The Red Rhino 2.0 is also configured to be equipped with rescue equipment which is more portable in nature. The hydraulic spreader and cutter equipment, previously powered by an on-board power unit, is now battery operated to allow greater flexibility in deployment during an emergency incident.

"The end result is a product which is 10% smaller and 40% lighter than the original version."

CONCLUSION

At that time, the idea of developing a new vehicle totally different from the existing appliances in service was considered radical and bold. The notion of omitting the water tank totally was also felt to be unimaginable by some officers. The then Commissioner of SCDF, Mr. James Tan, encouraged the

The concept of a fire-fighting vehicle – (left) latest Red Rhino developed in 2009 (middle) traditional fire engine or Pumper (right) first generation of Red Rhino developed since 2000

project team to re-visit and challenge the norms and assumptions of then current practice. This allowed the team to break tradition and conceive of the idea that eventually led to the birth of the Red Rhino.

In the last 10 years since its introduction, the Red Rhino has proven to be the SCDF's staple solution to combating nearly half of all fires in Singapore's dense urban environment. It has garnered awards such as PS21 ExCEL Convention 2000 – Gold, NQC Convention 2000 – Gold & PSB Eureka Award 2000.

Indeed, the Red Rhino has become the most recognisable "persona" that the Singapore public has come to associate with the SCDF today.

New generation of Red Rhino developed in 2009

First generation of Red Rhino developed in 2000

EDITOR'S NOTES

Teong How Hwa is a Lt Colonel in the Singapore Civil Defence Force (SCDF). He is presently seconded to MHQ/MHA as Deputy Director for Strategic Development.

The eVisitor Programme

MR. DAVID LEE TAI WEE

INCREASE IN DEMAND FOR VISITOR SERVICES

Foreigners call on the Immigration and Checkpoints Authority (ICA) to apply for a range of services from the extension of stay to the application of long-term or student's passes. In recent years, the visitor base has grown considerably. This can be attributed to the Singapore government's efforts to promote the country as a tourism, education and medical hub and Singapore's naturalisation efforts to augment the country's population.

The increase in demand for visitor services is amply evident in the rise of applications for Visit Passes and Student's Passes. In fact, there was an increase of 186 % from 220,000 applications in 2003 to 630,000 applications in 2009 (Figure 1). The increase in demand for visitor services resulted in a perpetual crowd at the Visitor Services Center (VSC) and put 'pressure' on ICA's staff and service delivery. Staff had to do overtime for much of the week. To address these challenges, the idea of developing the eVisitor Programme was born.

WHAT IS THE eVISTOR PROGRAMME?

The eVisitor Programme is a unique, integrated suite of online services to cater to the varied needs of increasing demand for visitor immigration services in Singapore. The eVisitor Programme is interfaced with validation portals and border control systems to provide visitors with a totally seamless service when visiting Singapore. It aims to facilitate a foreigner's stay in Singapore by providing online immigration services ranging from their application of entry visa and application of additional facilities whilst in Singapore to their departure from Singapore. Figure 2 shows the slew of the key online services available in the programme and how they are interfaced and integrated to achieve the ease and convenience that bona fide visitors' experience.

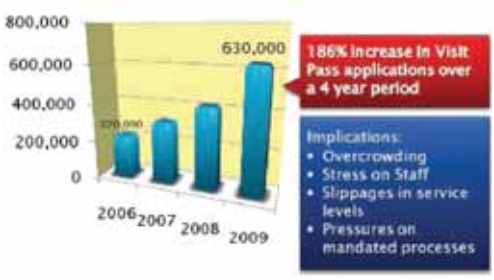


Figure 1 – Increases in Visit Pass applications over a 3-year period

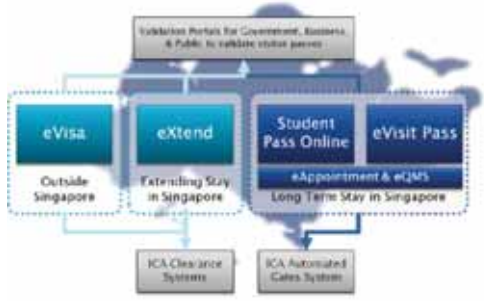


Figure 2 – Key Online Services under the eVisitor Programme

SERVICE INNOVATION

PREVIOUSLY, MOST OF the services at VSC were accessed by customers through the physical channels. These physical channels required comparatively more resources than that of the self-service and virtual channels. Hence the impetus to minimise the physical channels and contact time with customers. To do this, ICA recognised the need to leverage on technology to bring service into the 'virtual world' and to engage and empower partners to provide alternative "service windows" in order to bring convenience and added value to its customers.

It was not easy to implement. It was not merely replicating the 'old or physical procedures' into the virtual or online world. It required radical thinking, challenging entrenched ways and paving new ways of doing things. Fundamental questions were asked before embarking on the Programme – Why should security and service be mutually exclusive? Why can't both be achieved together? Does a visitor need to come to ICA in the first place? Do we need to have sight of his passport? Do we need to make physical endorsements on the passports? Can we work with partners to extend our presence beyond the ICA premises?

OUR VALUE PROPOSITION

Innovative and Novel Approach – Manual versus Online Process

IN THE PAST, visitors who applied for a short extension of stay in Singapore would need to visit ICA along with his/her local sponsor and fill out a 4-page declaration form before submitting the application over the counter. The applicant and sponsor could expect to spend almost a whole day travelling to ICA and waiting for an outcome which comes in the form of a physical endorsement on the passport.

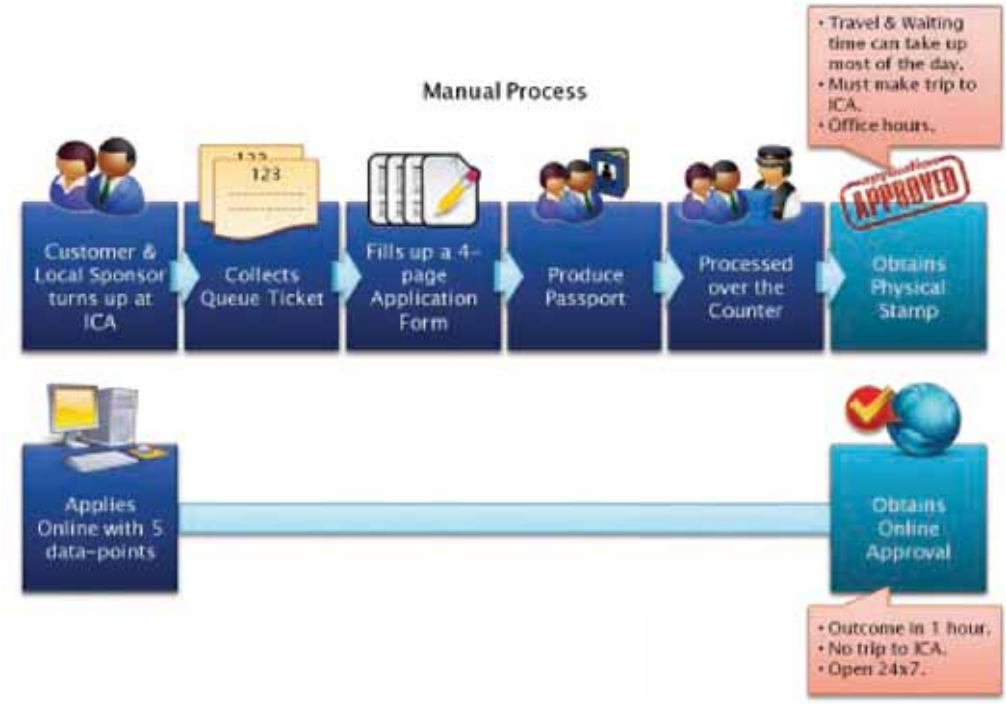


Figure 3 – Comparison between Manual and eVisitor process for Extension of short Stay

In early 2007, the VSC introduced an online application portal called *eXtend*, as part of the eVisitor Programme to facilitate short-term extensions for foreigners in Singapore. ICA took this step on the premise that most foreign visitors were genuine and that they were generally of lower immigration risk compared to customers applying for long-term stay to reside or study in Singapore. With this mental model, ICA took a radical approach in designing the *eXtend* portal by doing away with steps and requirements that were traditionally required by immigration authorities all over the world. These included doing away with the need for having a local sponsor and doing away with the need for the applicant to appear in person in ICAB for the application. In the process, we also did away with the old established practice of granting the outcome of stay via a physical endorsement in the passport. So, when the *eXtend* portal was introduced, almost overnight, tens of thousands of visitors and local sponsors no longer needed to make a trip to ICA to complete the application form to apply for a short extension of stay in Singapore. Instead, the applicant can now apply for extension in the comfort of his accommodation, at any time of the day (*eXtend* is available 24 hours a day, 7 days a week).

While handling the intricate aspects of staff sentiments in moving on to the new platform, we also had to manage the shift of staff mindsets to the new mode of delivering

immigration services to visitors online. This is particularly so since many officers traditionally relied on face-to-face checks for appearances of the visitor, checking on his passport and physical supporting documents (if any) to assess whether to grant the immigration facility to foreigners.

User-Friendly and Hassle-Free

THE SYSTEM WAS designed to be user-friendly and convenient. The customer only needs to key in 5 data points for the online application. This is a far cry from the past where they were expected to manually fill up a 4-page application. All the particulars of the applicant are instead obtained from the checkpoint database (which comprises among other particulars of applicant, a scanned copy of his/her travel document's bio-data page and his/her photo) when he/she first arrived at the checkpoints.

The *eVisa* system is another online service introduced under the eVisitor Programme that adopts an innovative and novel approach, challenging conventional wisdom that a visa must only be issued in the form of physical label (visa label) on the passport. Under *eVisa*, the local contact and applicants no longer need

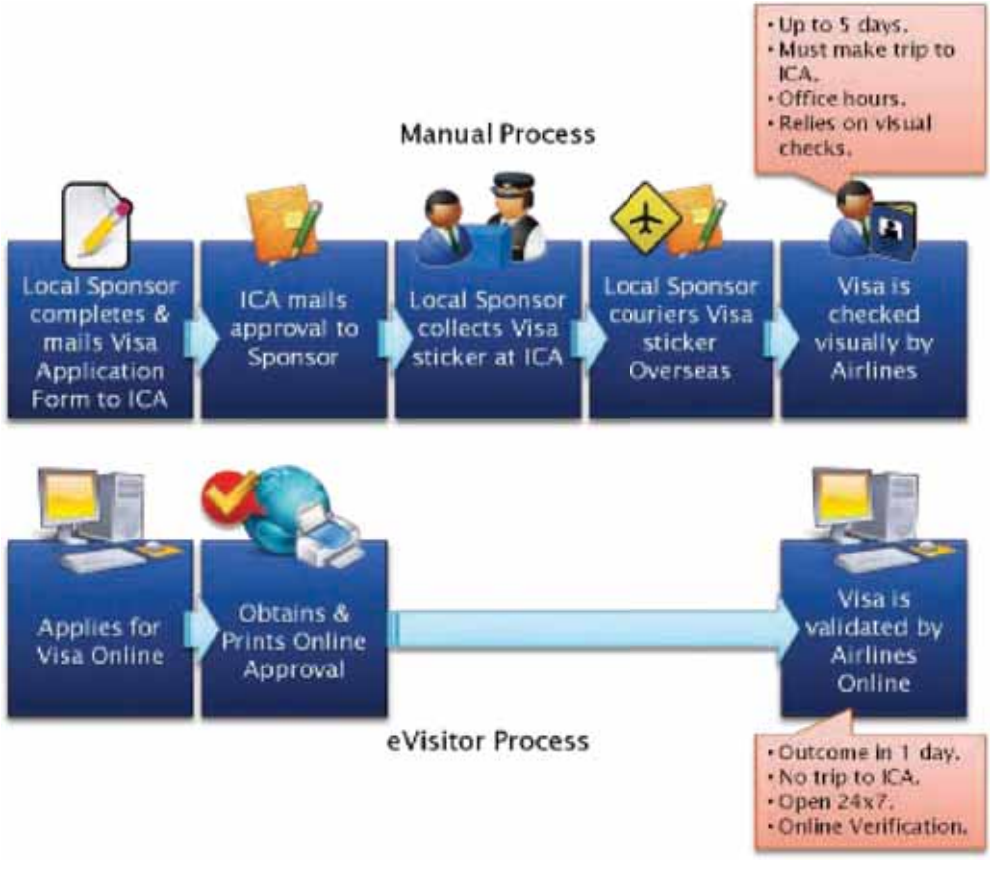


Figure 4 – Comparison between Manual and eVisitor Process for Application of Visa

to make a trip to ICAB or Missions to queue up to collect the approved visa label. They are now able to print the approved visa online anytime/anywhere, and fly to Singapore.

Faster Turnaround Time for Applications

LIKE THE SLEW of online services under the eVisitor Programme, the *eXtend* and *eVisa* are equipped with a customisable, complex rules engine so that it can automate the decision-making for legitimate cases using the retrieved data, and generate an approval (or a denial) online without any or only minimal human intervention. *eXtend* will return a result that the applicant can receive the approval online within an hour.

Targeted Approach and Enhanced Security

DESPITE ITS FRONT-FACING, service-oriented nature, the eVisitor Programme was designed with security in mind as well.

The introduction of online services under the Programme gave ICA the opportunity to introduce 'auto-rules engine' into its work processes. The system will flag out suspicious, high risk applications for closer scrutiny, while allowing the 'remaining' – aboveboard cases – to be approved swiftly with minimal intervention. This redeployment of limited manpower resources to process the more complicated and higher risk cases, allowing VSC to achieve a 40% increase in detection of dubious and multiple identity cases.

The eVisitor Programme also improves border security, particularly for departure clearance. In the past, checkpoint officers relied on endorsements on passports during departure to verify whether a visitor has not overstayed. Validation of these extensions stamps was difficult without intimate knowledge of ICA's stamps and their security features. (For illustration, two visit-pass endorsements are reproduced in Figure 5 to illustrate the challenge of telling the well-forged endorsement and the genuine one).

An important feature of *eXtend* over the traditional process was doing away with the physical endorsements /visit pass extension stamps entirely. When the visit pass extension is given online to the visitor, ICA's checkpoint systems would also be updated of his extension records. The visitor only needs to produce his passport and disembarkation-embarkation

Figure 5 – Before eXtend, officers would physically check extension stamps to verify whether they are forged (left) or real (right)

(DE) card upon departure and the system will automatically validate/verify whether the stay is legitimate or otherwise. In summary, with *eXtend*, there is no endorsement, and verification can be done online.

The eVisitor Programme also improves inland enforcement efforts. While some of ICA's own officers and strategic partners (such as fellow enforcement agencies) initially had reservations and raised concerns on how to check a foreigner's stay if there is no physical immigration endorsement in the passport, the Programme's implementation revealed the advantage of verifying the immigration status of a foreigner online. For example, a Home Team officer conducting checks on foreigners in Singapore on the streets can convey the person's passport details back to his counterpart in office with access to ICA's validation portal. This verification is more reliable as it is far less likely to be compromised compared to a physical endorsement.

Hence, by doing away with the physical endorsement on the passport and providing online verification instead, the Programme has reduced the opportunity for syndicates to use forged or tampered endorsements to facilitate the entry or departure of undesirables and prolonging their stay in Singapore.

Under the eVisitor Programme, the integrity of the system ensures data shown in the system is tamper-free compared to the integrity of the information endorsed or printed in the travel document or visa. With greater reliance on the data residing in the system, security is enhanced. The same concept of using online verification instead of plain physical examination is applied to *eVisa*, where the status of a visitor's visa can be checked online by the airlines, instead of relying on physical visa labels to validate the passenger.

Integrated and Seamless Service

The eVisitor Programme meets the increase in demand of visitor services not only through automation, but virtualisation of services. By placing application portals online, visitors will find it more convenient to access immigration services without the need to increase manpower and floor space to handle the substantial rise in traffic.

For long-term stay visitors (identified as long-term pass holders and student pass holders), visits to ICAB are still necessary to complete their biometric enrollment and verification of documents and certificates). In the past, Long Term Pass (LTP) holders used to come to ICA to apply for the pass, then again make a return trip to complete formalities, and collect the LTP card. When an applicant wants to apply for automated clearance

facilities, he/she would have to apply for this separately. Hence, in total, the applicant may have made up to 3 separate trips to ICA – i.e. to apply for a long-term pass, collect the long-term pass and sign up for automated clearance facilities.

Under the eVisitor Programme, a one-stop solution is offered instead. Applications can be done online and upon approval, applicants can make an e-appointment to come to ICA to collect their long-term pass. When collecting long-term pass card, applicants will automatically be eligible to use ICA's automated clearance system (eIACS) without additional effort on their part. The applicant effectively only makes one trip to ICA to obtain his card, with the added benefit of being able to enjoy automated clearance facilities without additional effort.

As a result of the crowd reduction and the electronic appointment booking system, the waiting times have reduced significantly in VSC. For example, the waiting time to complete formalities for the issuance of a long-term Visit Pass or Student's Pass was significantly slashed – from many hours to less than 30 minutes (non-peak periods).

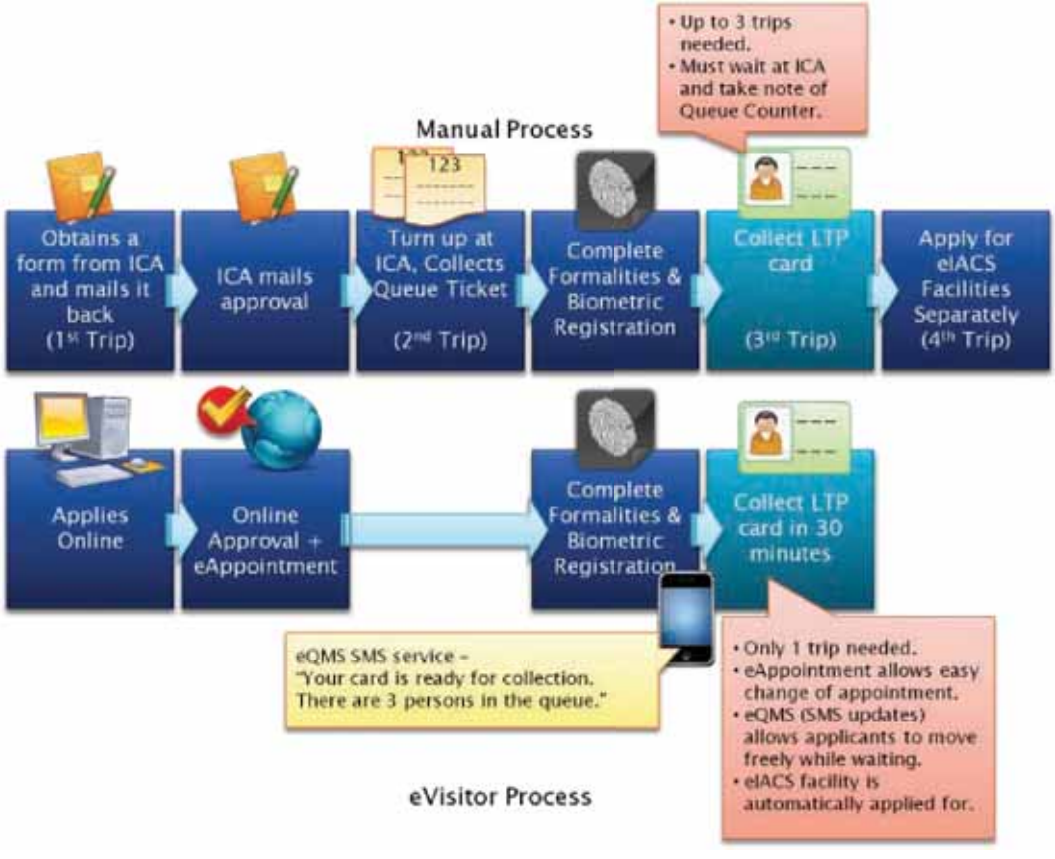


Figure 6 – Comparison between Manual and eVisitor Process for application of Long Term Pass (LTP) and automated clearance facility (eIACS).

ENGAGING PARTNERS TO CREATE ALTERNATIVE SERVICE WINDOWS – BRINGING SERVICE TO THE DOORSTEP

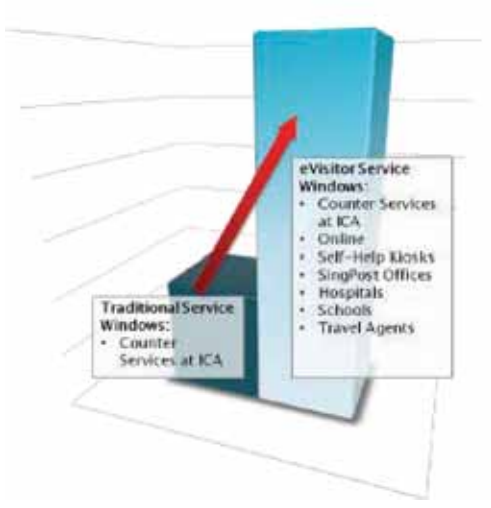


Figure 7 – eVisitor Programme pushes our services to alternate service windows to expand and extend the reach of our eServices

THE EVISITOR PROGRAMME provides an opportunity for ICA to work with strategic partners to create alternative service windows for immigration services. The review of existing services showed that not only can services be virtualised – they can also be handled by trusted partners.

As a direct effect of this realisation, ICA was able to work with Singpost to provide online assistance for visitors who need to access the slew of online services under the eVisitor Programme. This is especially beneficial for visitors who are not tech-savvy to apply for online immigration services by themselves (e.g. for a fee, Singpost will help the interested visitor apply for an extension of his stay). This not only reduces the need for applicants to come to ICA for assistance, it also increases the number of potential 'service windows' significantly – there are 62 Singpost outlets that provide such immigration services, and some of them even operate 7 days a week.

ICA also engaged trusted partners to create new value for their customers by 'empowering' them with access to apply for immigration services in lieu of the actual visitor. An example of how this benefits visitors – international patients who come to Singapore for medical treatment previously are required to apply for visa by themselves. After receiving treatment they would have to apply for extension of stay personally should their treatment require it. Any caregiver visitor would also have to do the visa applications and extensions by themselves.

Previously, the local contact or visitor is required to produce documents/medical memo from the local doctor or healthcare player to support the visa application or extension of stay in Singapore. As part of due diligence, ICA has in some cases contacted the doctor/healthcare provider to ascertain if the documents produced are valid and genuine. Now, under the eVisitor's Trusted Partner Programme, local hospitals and

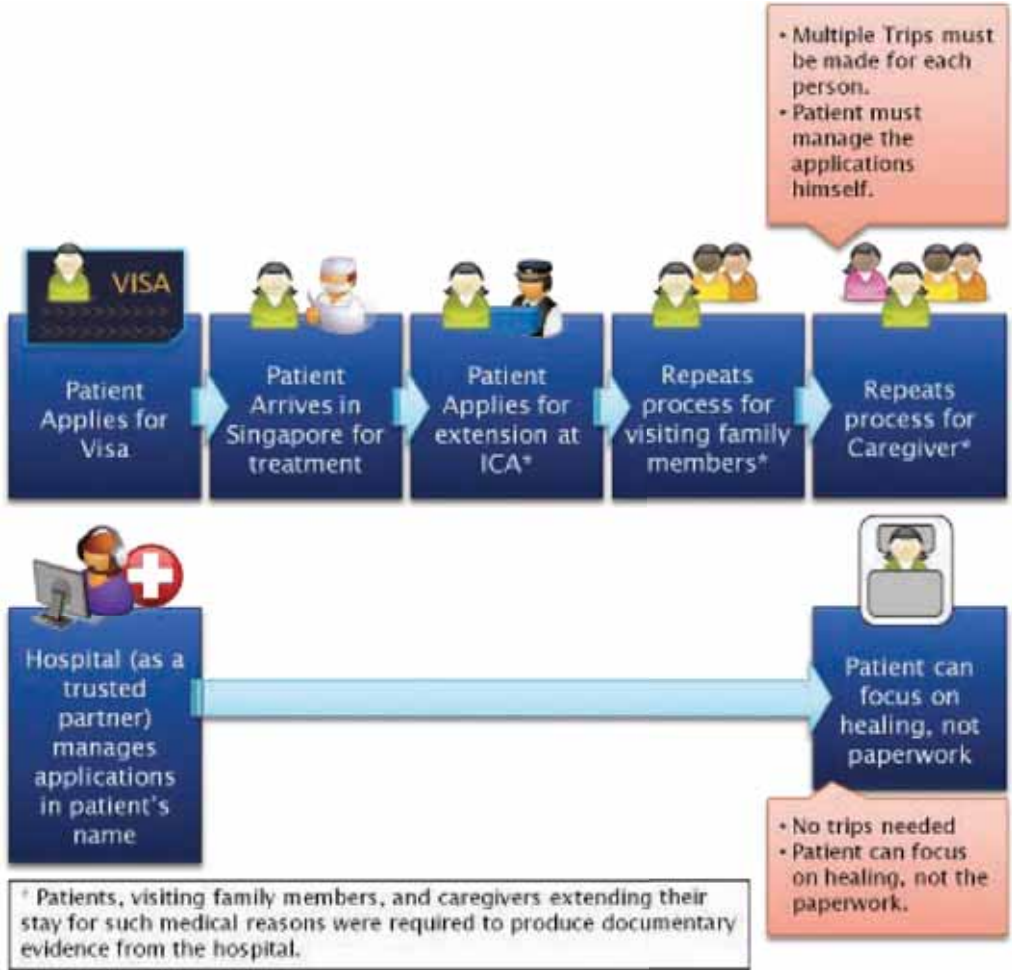


Figure 8 – eVisitor Programme enables partners to provide value-added services for their customers while serving as alternative service window, creating an all-win combination for ICA, the partner, and the visitor.

healthcare providers can apply a visa or extension of stay not only for their patients, but also his caregiver and relatives as well. This has made visa application and extension of stay for medical tourists both convenient and hassle-free. The patient is relieved of the paperwork and can fully focus on his recovery. This novel and hassle free approach has given our hospitals and healthcare providers the extra edge to draw medical tourists to Singapore and help augment Singapore's medical hub status.

"With all these time and cost savings, we are able to channel our marketing efforts to promote Singapore as the ultimate choice for International Patients to seek treatment.... They need not worry about these [immigration] matters."

Raffles International Patients Centre
Raffles Medical Group

IMPACT

Improved Public Perception

The introduction of eVisitor Programme has shown an improvement in the speed of services and public perception of ICA. Figure 9 illustrates the improved customer satisfaction results arising from a survey by Forbes over 3 separate periods (or waves) from 2006 to 2008.

Reduction of Crowds at ICA Building

The improvement is even more apparent by the easing of crowds in ICA's Visitor Services Centre (VSC) in the past 1 to 2 years. The Programme has drastically reduced the crowd at VSC as more than 80% of all applications to VSC are now made online. The number of visits made to ICA by customers has reduced by an average of 2,500 visits per day or 700,000 per year. This translates to a reduction of **1.5 million** trips per year to ICA by customers.

Cost Savings/Avoidance

The implementation of the Programme has helped achieve cost savings and cost avoidance for both ICA and the public.

ICA is able to achieve $1 million savings per year by doing away with physical visas, postage costs etc when the e-Visitor Programme was rolled out. ICA was also able achieve a cost avoidance of up to $2 million per year as ICA – costs that would otherwise be incurred to beef up manpower resources, expand VSC's operations area and related

Figure 9 - Customer Satisfaction Survey by Forbes

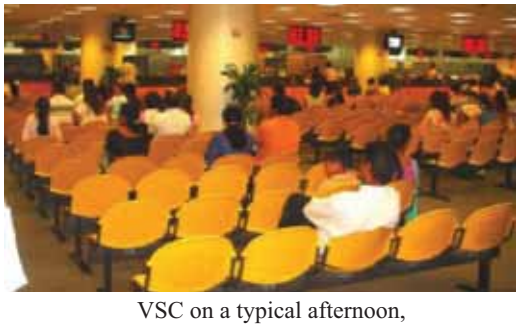
infrastructure /imputed rental costs to meet the increased demand for ICA's services by foreigners.

Moreover, customers were able to reap significant benefits too. They save up $4.5 million per year in terms of transportation costs as they could now make either 'zero' or just a single trip to ICAB for their immigration facilities – instead of making multiple trips in the past for such services.

Enhanced Security

By leveraging on technology to process cases with minimal human intervention and a faster turn around time, we were able to redeploy about 15% of the total staff strength to handle higher risk cases and contribute to value–added work. This saw an increase of up to 40% in the detection of cases of double identities and dubious applications by customers.

VSC on a typical afternoon, Before eVisitor Programme



VSC on a typical afternoon, After eVisitor Programme

AWARDS & ACCOLADES

The eVisitor Programme has won numerous awards, including the prestigious FutureGov/Government Technology Awards 2008 (an international competition featuring the best from Asia Pacific and the Middle East), the CIO Awards 2009, and the SiTF Awards 2009. It also participated in other international and national competitions:

- Winner, MHA 3i Innovation Awards Winner 2008
- Recipient, Minister National Day Awards 2009
- Finalist MIS Asia IT Excellence Awards May 2009
- Finalist UN Public Service Awards April 2009
- Finalist APICTA Awards December 2009

INSPIRING CONFIDENCE IN ALL

IN CONCLUSION, THE eVisitor Programme has significantly enhanced service delivery and brought ICA's services closer to their doorsteps by working with partners to provide numerous 'alternative service windows' to access the immigration facilities. ICA creativeness and collaborative approach has brought significant benefit and value to the customer in terms of costs and time. Yet it has also enhanced security while supporting national initiatives at the same time. This journey has also boosted staff morale by encouraging better work-life balance with less need to work overtime since work processes have been reduced and streamlined. The awards conferred to the eVisitor Programme is recognition of the excellent service consciousness and security focus of ICA – stamping our role as a world-class border security and identification organisation that renders services delighting the public and inspiring confidence in all.

"This journey has also boosted staff morale by encouraging better work-life balance with less need to work overtime since work processes have been reduced and streamlined."

EDITOR'S NOTES

Assistant Superintendent of Police (ASP) David Lee is a Technology Executive in the Technology Division of the Immigration and Checkpoints Authority (ICA). The ICA's eVisitor Programme recently won the Singapore Infocomm Technology Federation (SiTF) Awards in 2009.

APEC *Trojan* Email Attacks

MR. LOH PHIN JUAY

CYBER-ESPIONAGE IS THE theft of information, in particular classified government information, via cyber means. The high profile disclosure of *GhostNet* in March 2009[1] underscores the seriousness of the cyber-espionage threat in today's wired societies. Investigations into *GhostNet* found that over 1,000 computers belonging to various government offices, such as foreign ministries and embassies, of India, South Korea, Indonesia, Romania, etc., were successfully infiltrated through emails that contained malicious software, or malware. To date, the perpetrators of *GhostNet* remain unknown.

This form of cyber-espionage is commonly known as a Trojan attack. It refers to a malware that appears to be legitimate but facilitates unauthorised remote access to compromised computer systems instead. Although Trojan attacks depend primarily on the efficacy of a well-programmed malware to circumvent computer security detection and to execute the orders of its controller, a successful attack usually also involves crafty social engineering techniques. These techniques are aimed at masquerading the attacker's malware delivery as legitimate, either by spoofing the email as coming from a trusted source or enticing the recipient with interesting content either as a file attachment or web-link. Once hoodwinked to open the malicious file attachment or click the web-link to be directed to a malicious website, the malware is activated and the computer system is compromised. The attacker can then gain remote access to the system and will be able to view or download files on the victim's computer, monitor the victim's activities so as to gather passwords and other sensitive information, or to spread malware to others by posing as the victim. It is noteworthy to add that when protecting systems against Trojan attacks, no amount of IT security software and hardware can substitute for user vigilance when confronted with suspicious emails and attachments.

Trojan email attacks are not new to Singapore. Between 2004 and 2005, the Singapore Government saw several waves of Trojan email attacks which were commonly referred to as the Trojan Riler[2] attacks. In four waves of attack over a span of 2 years, civil servants in several ministries

were targeted. The emails sent by the perpetrator(s), totalling more than 900, typically contained relevant news and information from the Internet in order to entice the recipients to open up the emails and their malicious attachments.

Such attacks are opportunistic and often leverage on the window of opportunity resulting from unpatched security flaws within a computing software or hardware. Therefore, adopting a holistic approach towards IT security is key. This necessitates cautious assessment and evaluation of the potential risk, at times, taking into consideration the worst-case scenario (that a compromise to the system will definitely occur!). By doing so, sound safeguards and controls could then be built in to prevent loss of any sensitive data even if the systems become infected.

"There were at least 7 waves of attacks between September and November 2009."

TROJAN ATTACKS DURING APEC 2009

IN THE LEAD-UP to the recently concluded Asia-Pacific Economic Cooperation (*APEC*) 2009 meetings held in Singapore, purposely crafted emails from attackers impersonating as Singapore government officials of the APEC 2009 Organising Committee were sent to APEC officials and delegates of various APEC economies, with the aim of infiltrating their computers and extracting privileged information. There were at least 7 waves of attacks between September and November 2009. The attacks were highly targeted, focusing on members of the APEC Organising Committee and APEC delegates whose email addresses were published on various APEC websites, or found within APEC mailing lists.

In one of the first waves of Trojan attack, the perpetrators sent an email warning Singapore civil servants involved in the APEC meetings of impending terrorist attacks. The perpetrators further provided photos of supposed terrorists in a Microsoft PowerPoint document which was infected with the malware. They played on the heightened security consciousness of the government officials to trigger and execute the malware, thus infecting the targeted computer systems. This modus operandi was repeated in at least one other Trojan attack on APEC 2009 delegates, but using a different subject matter and using an Adobe PDF document to host the malware.

In another Trojan attack, social engineering techniques were again used, but in a slightly different way, to try to trick APEC delegates into opening an email and executing an infected attachment. Analysis of this attack surfaced that legitimate information relevant to the APEC 2009 meetings was exploited to craft the attack email. Using the information as a cloak of legitimacy, in this case, details of an actual APEC symposium, the perpetrators masqueraded as a Singapore official to invite several

APEC delegates to the symposium. Thinking that the email was genuine, APEC delegates who opened the email and its attachment had their computers infected with the malware.

MALWARE ANALYSIS: BEHAVIOUR AND COMMUNICATION PATTERNS

THE MALWARE USED in these attacks were highly sophisticated and stealthy enough to evade the detection of most anti-virus programmes. Testing of the malware surfaced that the Trojan would call back to the attack-control server on a regular basis to receive instructions. Once the instructions were received, more malware would be executed on the infected system. The Trojan allowed the attackers access to all the files in the compromised computer, monitor its activities and communications, obtain usernames and passwords, and essentially take full control of the victim's computer.

PROFILE OF PERPETRATORS: INTERESTS AND TECHNICAL CAPABILITIES

THE PERPETRATORS WERE interested in contact information such as emails, Microsoft Word, PowerPoint, Excel and Adobe PDF documents. Besides being potentially-useful intelligence, these documents were also likely useful for the social engineering required for subsequent attacks. The perpetrators were also interested in obtaining usernames and passwords for web-forums and webmail services; they executed an application to extract cached email passwords from a number of email clients such as Microsoft Outlook, Gmail and Hotmail. The attackers scanned the infected system's network setup and configuration, version of Microsoft Office installed, computer services running and programmes installed, so as to understand the computer's vulnerabilities. Understanding such vulnerabilities would facilitate the perpetrators in executing attacks on other computers residing in the same network.

The perpetrators were technically savvy and demonstrated security consciousness. Other than deleting their traces in the infected computers after they had finished their operations, they also established anti-tracking operational set-ups, for example, their control servers were registered with fake names just prior to the attacks, and likely to be used purely for controlling the Trojans and discarded after the attacks were completed. Analysis of the communication between the malware and the control servers led to dubious domain names and registrants.

SITSA'S ROLE IN MITIGATING THE APEC TROJAN ATTACKS

SINGAPORE INFOCOMM TECHNOLOGY Security Authority (SITSA), as the dedicated and

specialist authority undertaking the responsibility of operational IT security at the national level, worked with Infocomm Development Authority (IDA), which is responsible for cyber security within the government sector, to identify the relevant malware characteristics needed to put up countermeasures. IDA focused on the immediate incident response activities while SITSA put its resources to work on investigating the attacks and addressing other potential threats arising from these attacks. For example, some of the malicious emails contained details of actual APEC events (date, time, venue) not known to the general public. That attackers' access to such information could potentially threaten the smooth running of those events. This piece of information was promptly shared with other security agencies to ensure that any potential threat was properly assessed and mitigated.

CONCLUSION

IN THIS INCIDENT, the Singapore government suffered minimal damage, and this was due in part to lessons learnt from previous cyber incidents and also the close cooperation between SITSA and key stakeholders such as IDA.

The cyber-threat landscape is ever-evolving and we will not be seeing the last of such cyber attacks. Lapses and complacency may bring about a 'Digital Pearl Harbour' to the nation. While it is not possible to prevent 100% of all attacks from succeeding, the key to minimising and mitigating this increasing number of sophisticated attacks and its consequences is a holistic strategy that involves the cooperation of all stakeholders, in particular system owners, who must not forsake IT security measures and best practices because of reasons such as user-convenience and the ease and cost of implementation.

EDITOR'S NOTES

Mr. Loh Phin Juay heads the Singapore Infocomm Technology Security Authority (SITSA) section that responds to and manages cyber incidents. SITSA was set up in 1 Oct 2009 to safeguard Singapore against Infocomm Technology (IT) security threats. It is the national specialist authority overseeing operational IT security. SITSA's mission is to secure Singapore's IT environment, especially vis-à-vis external threats to national security such as cyber-terrorism and cyber-espionage.

Technology Crime Forensic Branch: *Hitting the Hard Drives*

MS. CONNIE SEEK

OUR HUMBLE BEGINNINGS

In 1997, the Computer Crime Branch (CCB) was established as part of the Commercial Crime Division (CCD) of the Criminal Investigation Department (CID) at the old CID Building at Eu Tong Sen Street with only four investigation officers.

With rapid development of computer technology in the 1990s, CCB evolved to become the Computer Forensic Branch (CFB) in 2000 before it expanded to become the Technology Crime Division (TCD) on 15 October 2001 to serve as an investigation, response and computer forensic processing entity for the Singapore Police Force (SPF).

Today, the TCD consists of the Technology Crime Investigation Branch (TCIB), Technology Crime Forensic Branch (TCFB) and Technology Crime Research Branch (TCRB) with a total of about thirty officers. This is a far cry from when we started as CCB in 1997.

TCIB serves as an investigative arm to all offences classified under the Computer Misuse Act while TCFB serves as a technology forensics processing entity to aid SPF and other local law enforcement agencies in the criminal investigation process. The branch also serves as the staff authority on technology forensic matters. Last but not least, TCRB was formed with the objective to tackle technology crime proactively.

TCFB'S VISION

TCFB endeavours to be the cutting edge in technology crime fighting and to be the premier unit in technology forensic investigation.

Technology Crime Forensic Branch at Police Cantonment Complex

ORGANISATION SET-UP OF TCFB

TCFB is a very small branch that is made up of only two teams of technology forensic examiners and Technical Support Officers. Each team is supervised by an OC Team who also assists Head TCFB to plan, oversee, provide leadership, and devise strategies and counter-measures for the overall operational effectiveness of the TCFB. The branch reports directly to 1 Deputy Director CID.

CORE CAPABILITIES OF TCFB

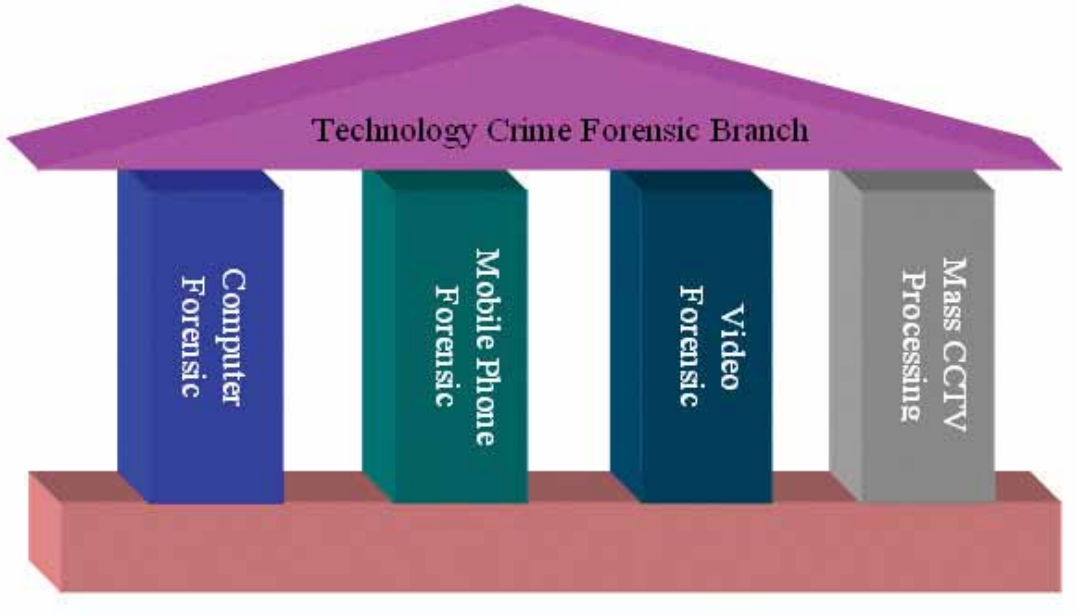
TCFB has four capabilities broadly classified as Computer Forensic, Mobile Phone Forensic, Video Forensic and Mass CCTV Processing.

TCFB has adopted the various best practices from other law enforcement forensic experts and agencies over the years such as the Association of Chief Police Officers (ACPO) guidelines in the handling of electronic evidence in maintaining a proper chain of the exhibit custody, and to ensure the integrity of the electronic evidence.

What Is Computer Forensics?

Computer Forensic was officially rolled out in 2001. It refers to the collection, preservation and analysis of electronic data found in computers and digital storage mediums in a systematic and scientific manner to uncover digital evidence.

In the area of computer forensic, TCFB officers are trained to handle and extract evidences from storage



devices such as hard drives from desktops, laptops and portable devices such as thumb drives and storage cards.

TCFB uses a variety of commercially available computer forensic softwares to conduct analyses on the exhibits. Some of the common computer forensic requests that TCFB received includes:

1. Retrieval of 'live' and 'deleted' documents/pictures/ videos of various formats;
2. Retrieval of internet activity logs e.g. Internet history, Internet cookies, emails exchanges, chat logs etc;
3. Retrieval of system information logs e.g. Operating System, hardware and software information, network settings, logged-in user history etc;
4. Data carving from hard disk 'unallocated space'; and
5. Simple password cracking.

What Is Mobile Phone Forensic?

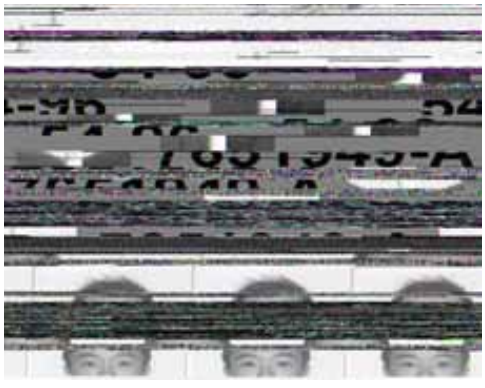
Between 2003 and 2004, TCFB operationalised its mobile phone forensic capability. Mobile phone forensic refers to the collection, preservation and analysis of electronic data found in the mobile phone in a systematic and scientific manner to uncover digital evidence. It usually involves the examination of the mobile phone handset, the Subscriber Identity Module (SIM) card and the attached storage media.

There are a wide variety of operating systems used by different

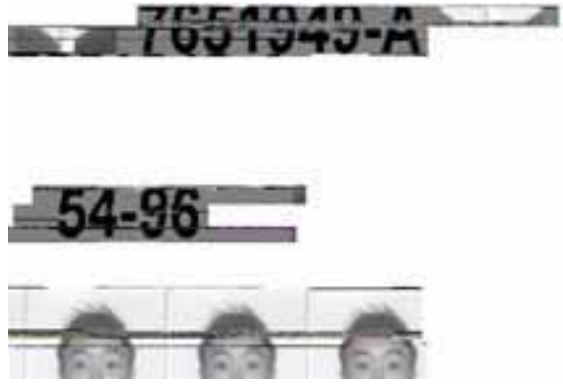
Handset Interrogation

SIM Card Interrogation

Memory Card Interrogation



File fragment found in unallocated cluster



Repaired file

models and brands of mobile phones. Hence, mobile phone analysis has to be conducted using different mobile phone analysis softwares. TCFB had procured different commercial mobile forensic softwares to support mobile phone analyses. TCFB's mobile phone forensic capabilities include:

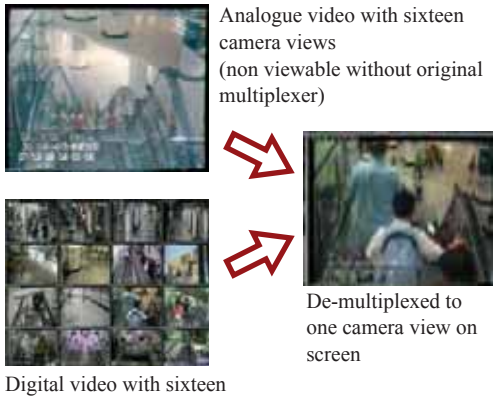
1. Retrieval of 'live' or 'deleted' SMS, pictures, files and videos from mobile phone, SIM card and add-on memory storage;
2. Retrieval of call history e.g. dialled numbers, missed calls, received calls from mobile phone and SIM card; and
3. Retrieval of phone book records from mobile phone and SIM card.

What Is Video Forensic?

VIDEO FORENSIC IS the other forensic capability in TCFB that was rolled out together with the mobile phone forensic capability in 2003 to 2004 following the proliferation in CCTV camera coverage in both public and private places. Video forensic is the examination, comparison and/or evaluation of video footages to uncover digital evidence. Video evidence from the CCTV recordings had proven to be a strong supporting lead in many of the serious crime investigations.

Some common video forensic techniques that are deployed by TCFB are:

1. Digitising video tape footage;
2. Converting digital videos from DVR devices into digital video formats usable for forensic analysis;
3. Separating camera views from multiplexed CCTV footages;
4. Performing clarification techniques e.g. Frame Averaging and Image Enhancement;
5. Highlighting subject of interest in the video e.g. crime sequence recreation; and
6. Enlarging or capturing screen shot of portions of the video as areas of interest.



Technique of separating multiplexed CCTV footage

What Is Mass CCTV Processing?

MASS CCTV PROCESSING is a contingency capability rolled out by TCFB in 2006 following the success of the UK

Metropolitan Police's CCTV trawling operation to establish the identities of the perpetrators in the immediate aftermath of the London Bomb Blast on 7 July 2005.

It refers to the behind-the-scene processing of large volumes of CCTV footages, which may include multiplexed footages or proprietary digital formats, to a 'viewable' format for the facilitation of mass CCTV viewing by the Investigation Officers at the TCFB Simulation Laboratory in the immediate aftermath of a bomb blast incident.

The ability of TCFB to process seized CCTV footages into a 'viewable' format helps to provide timely investigation leads for Investigation Officers, which is critical to the success of the identification and apprehension of the perpetrators after a bomb blast incident. Since 2006, TCFB has worked closely with CID's Operations & Investigation Policy Branch and the Public Transport Operators (PTOs) in Singapore to build up the capability to process any CCTV image seized from the PTOs in the event of a bomb blast incident that occurred at a public transport facility. This capability was exercised in Exercise NorthStar V on 8 January 2006 and in CID's in-house post-blast investigation exercise, Exercise Storm III GDX, on 3 September 2007.

CHALLENGES FACED BY TCFB

TCFB's FORENSIC WORK is compounded by the unique complexities of each stage of its forensic processes. The fast evolution of technology (e.g. development of bigger capacity for hard drives, prevalent usage of encryption software, and enlargement of different types of exhibits which need to be seized by IO) also added complexities to the forensic processes.

All exhibits received by TCFB need to go through a forensically sound process of acquisition so that an image copy of the original electronic data is acquired to allow the forensic examiner to examine the imaged electronic data as if it were the original data. However, not all exhibits come to TCFB physically sound. Some exhibits are deliberately

CCTV footages of perpetrators obtained by London Metropolitan Police's CCTV trawling operation for the London Bomb Blast on 7 July 2005

Mass CCTV Viewing at TCFB Simulation Laboratory after processing by TCFB

damaged by criminals in a bid to destroy evidence while others are already in poor physical conditions resulting in read-sector errors during the acquisition process or lengthened acquisition time. The exhibits have to be dismantled carefully to reveal the storage devices, which are sometimes hidden, without causing further damage to them.

It is often misconstrued that the forensic processes are entirely automated, rudimentary and can be completed quickly. The analysis of the forensic data is actually a manual process performed by the forensic examiner. It has become increasingly common to receive an exhibit computer system that contains more than one hard drive or a hard drive with a storage capacity of 1 to 1.5 terabyte. As a result, the manual analysis is fast becoming more tedious and time-consuming compared to the past as the forensic examiner will need to go through a larger volume of data.

Investigation officers are also misled by television crime dramas such as the 'CSI: Crime Scene Investigation' and have unrealistic expectations on how far technology forensic can be used to support their investigation. For example, many people were misled that all CCTV footages or images could be enhanced to the same degree of clarity they saw on crime dramas without realising that the degree of enhancement relies on the quality of the image or video source.

ELECTRONIC DATA IS NEVER ERASED

IN THE ELECTRONIC world, data is never simply erased at the click of the 'delete' button. This has been extremely helpful in uncovering the

Damaged laptops sent to TCFB for forensic examination – exhibits were thrown down a flat by unlicensed money lenders

wrongdoings of Anthony Ler Wee Teang who manipulated a 15-year-old teenager to stab his wife on 14 May 2001.

TCFB forensic examiner uncovered nine Microsoft Word documents deleted in Anthony Ler's home computer that revealed a 'silent' conversation between him and his accomplice, three days after the death of his wife. Using these deleted files, police was able to prove that Anthony Ler used his computer to communicate 'silently' with the teenager at his flat. Some lines in the deleted file included "They can hear what you are saying", "Act shock that the woman is my wife", "Payment might have to wait" and "Yu threw the knife".

Anthony Ler was found guilty for the abetment of the murder of his wife and sentenced with the death penalty. The 15-year-old teenager was sentenced to indefinite detention in lieu of the death sentence.

COMBINING ELECTRONIC EVIDENCE WITH DETECTIVE SKILLS

ALTHOUGH ELECTRONIC EVIDENCE played a key part in convicting Anthony Ler for plotting the murder of his wife, it was not the only piece of evidence that police had against him. Very often, the good old detective skills still have to be applied together with electronic evidence to solve a case.

On 11 April 2003, Suresh Nair Vellayutham, a 28-year-old Malaysian working in Singapore, was arrested for aggravated sexual offences committed against two Indonesian air stewardesses at the Grand Hyatt Singapore hotel on 8 April 2003.

PRIME NEWS

Man offered killer $100K, court told

Murder trial hears that ex-Web designer Anthony Ler plotted his estranged wife's murder and lured teenager to do the job

LER IS ON TRIAL FOR MASTERMINDING THE MURDER AND FACES THE DEATH PENALTY. THE BOY IS CHARGED WITH MURDER BUT, AS A

PRISONS

ANTHONY LER & TEEN'S TRIAL

Prosecution: Afraid of being overheard...

They used computer to talk

Boy: I was pressured to kill

Newspaper clue in case

A piece of electronic evidence – a photograph of a lady in an airline uniform – recovered by TCFB from a memory card left by the accused at the crime scene led the police to solve the case successfully.

Through relentless detective works, police traced the lady in the photograph to her workplace and subsequently established the accused to be her boyfriend. Witnesses' testimonies also revealed that the accused was seen waiting in the hotel lobby and had claimed that he was waiting for some airline staff when he was questioned by a duty manager from the hotel.

The hotel's CCTV also captured his movements at the hotel lobby of him following the two victims into the lift and out of the lift. The accused's photographs were also recovered by TCFB from the memory card left at the crime scene. All these corroborated with the electronic evidence from the memory card misplaced by the accused at the crime scene.

Suresh Nair Vellayutham was found guilty of five charges – one count of rape and four counts of aggravated molestation. He was sentenced to twenty-six years of jail sentence and twenty-four strokes of the cane.

CCTV evidence corroborated with the electronic evidence recovered from the memory card to place the rape accused at the crime scene

HOME

Rape accused traced via camera card

At hotel crime scene, he allegedly left behind memory card which had photos of his girlfriend wearing airline uniform

'Evidence' found in room

Photograph of a lady in an airline uniform was recovered by TCFB from a memory card left at the crime scene – It led the police to establish the identity of the rape accused through subsequent detective works

TAKING A PROACTIVE APPROACH

SINCE 2006, UNPRECEDENTED demands were placed on TCFB to support SPF in the area of investigation into crimes, major incidents and public order situations related to the conduct of the S2006 International Monetary Fund/World Bank Group Meetings, ASEAN Summit 2007, Formula 1 SingTel Singapore Grand Prix and the Asia-Pacific Economic Cooperation (APEC) Singapore 2009 Meetings.

Set against the backdrop of a heightened security and public order threat climate, TCFB was driven by the need to ensure that its capability of Mass CCTV processing can support a post-incident follow-up. This is especially so when some incidents took place during these high profile events were captured by CCTV systems. To ramp up the Mass CCTV capability in preparation for these events, TCFB would devote much of its resources to conduct CCTV terrain mapping in the event localities before the start of each event.

The CCTV terrain mapping is a tedious and time-consuming process that requires TCFB to visit each estate owner in the event localities and their respective CCTV vendors to understand the CCTV systems. For example, TCFB spent an average of one month to conduct CCTV terrain mapping before the start of the Formula 1 SingTel Singapore Grand Prix each year. During the mapping exercise, TCFB will collate the CCTV technical specifications, including the software players, CCTV layout plans from the CCTV owners and vendors through ground visits. The information collated from the mapping exercise is critical for CCTV Mass Processing due to the large number of proprietary digital video formats used.

FLYING TCFB'S FLAG HIGH

SINCE THE INCEPTION of TCFB in 2001, we worked tirelessly to make a name for ourselves as the premier unit in technology forensic investigation in the region. We finally had an opportunity to participate in an INTERPOL mission in 2008.

On 7 March 2008, a TCFB forensic examiner, Senior Staff Sergeant (SSSgt) Joe Ng, was deployed as part of the INTERPOL Computer Incident Response Team to Bogota, capital city of Colombia.

The INTERPOL Computer Incident Response Team was requested to examine laptops and storage devices recovered following a raid on a terrorist camp belonging to the Revolutionary Armed Forces of Columbia (FARC) on the Ecuadorian side of its border with Columbia on 1 March 2008.

The raid resulted in the death of Raul Reyes who was the No. 2 man of the FARC. Colombia claimed that there were documents in the computers that indicated that Ecuador is supporting the activities of FARC. Ecuador, on the hand, claimed that the document could have been inserted by Colombia's authority. This raid created a border tension between Colombia, Ecuador and Venezuela.

The task assigned to SSSgt Joe Ng and another Australian technology forensic expert was to examine the laptops and storage devices to determine whether any data had been edited after the raid carried out by the Colombia's authority. SSSgt Joe Ng and his teammate spent more than 1,000-man hours going through more than 600GB of data. The forensic findings were submitted to a panel of Computer Forensic Experts for evaluation and the panel agreed with the forensic findings of the technology forensic examiners that there was 'no evidence of modification, alteration, addition or deletion' in the user files on the computers seized.

ASEAN LEAD SHEPHERD FOR CYBER CRIME FIGHTING

SINGAPORE WAS APPOINTED the lead shepherd for the ASEAN fight against cyber crime in 2004 at the ASEAN Ministerial Meeting on Transnational Crimes (AMMTC) in Bangkok, Thailand. As the lead shepherd, Singapore's responsibility is to create awareness and enhance general cyber crime fighting capability among the ASEAN members. TCD is the main driving unit behind the lead shepherd's role for cyber crime. Together with TCIB, TCFB introduced some initiatives such as the organisation of the bi-annual Cyber Crime Investigation Course (CCIC) and Cyber Crime Investigation Workshop (CCIW). To date, TCFB has conducted two runs of 2-week working attachment for the Royal Brunei Police Force (RBPF) in August 2008 and June 2009.

In addition to the rolling out of various training programmes for the ASEAN countries, TCFB has also put up a project paper to assist some ASEAN countries to set up basic technology forensic capability to help enhance their cyber crime fighting capability. This project is currently pending funding from dialogue partners through the ASEAN Secretariat.

For 2009, in line with our role as the lead shepherd for ASEAN cyber

crime fighting, TCD also worked with the SCTIP (Service de Coopération Technique Internationale de Police) to conduct the second Regional Cyber Crime Seminar 2009 from 23 to 25 November 2009. The theme of the seminar was 'Combating the Threats of Cybercrime and Financing Terrorism. A total of thirty-five participants from Singapore (SPF, Attorney-General's Chambers, Ministry of Home Affairs, Singapore Armed Forces), Hong Kong, South Korea, Japan and eight other ASEAN countries (Malaysia, Brunei, Thailand, Philippines, Laos, Vietnam, Cambodia and Indonesia) attended the seminar. The speakers included French Justice and Police representatives and World Bank consultants. The first Regional Cyber Crime Seminar was successfully carried out from 24 to 26 April 2007.

"With the increasing demand for digital forensics, TCFB will continue to harness innovative technologies to meet the challenges of bringing about stronger evidence for prosecution in future."

CONCLUSION

TCFB has come a long way since its inception. With the limited staffing, we have achieved much in the eight years since commencing operation to fulfill our mandate in ensuring that SPF has the competency to deal with technology-related incidents effectively and efficiently.

With the increasing demand for digital forensics, TCFB will continue to harness innovative technologies to meet the challenges of bringing about stronger evidence for prosecution in future.

EDITOR'S NOTES

Assistant Superintendent of Police (ASP) Connie Seek is Officer-in-Charge of a Team within the Technology Crime Forensic Branch (TCFB) of the Criminal Investigation Department (CID). She oversees a team of six Technology Forensics Examiners and one Technical Support Officer to carry out technology forensics examination to support frontline investigation officers in the Home Team.

Thinking *about the* Future:

What the Public Service Can Do

MR. PETER HO

IT IS FAIR to say that Singapore recognises the need for decision-makers to prepare for the future. Our efforts to understand and plan for the future have evolved and improved over the years. Scenario planning is now a key part of the Government's strategic planning process, and has proven useful in surfacing otherwise hidden assumptions and mental models about the world. More importantly, the scenario planning process has helped to inculcate an "anticipatory" mindset in many of our civil servants by getting them to raise "what if" questions on the issues that they deal with. The Risk Assessment and Horizon Scanning programme (or RAHS), launched in 2004 as a complementary capability to scenario planning, is being used to examine complex issues in which cause and effect are not easily discerned; it also serves as a shared platform for analysts from different agencies to collaborate on perspective-sharing, modelling and research.[1]

Yet why do decision-makers, who have ready access to ample information, fail to respond to warning signals of imminent crises? Why, despite support from the public sector leadership, and years of scenario planning workshops, and with new tools like RAHS, are we still not fully adept in anticipating the future? How can government agencies better organise their strategic thinking about the future?

We miss out on signals not only because of the limitations of our tools and methods, but also because of the nature of human cognition.

OBSTACLES IN ANTICIPATING STRATEGIC SURPRISES

THE HUMAN MIND can play tricks on us. We see what we want to see, and sometimes miss out the glaringly obvious. So it is with thinking about the future. We miss out on signals not only because of the limitations of our tools and methods, but also because of the nature of

human cognition. Many surprises that governments have to deal with – natural disasters, pandemics, even financial crises and political upheavals – can often be assigned probabilities, or anticipated through the "stories" or "narratives" that scenario planners use. This should lead governments to take precautionary measures. The reality is that we often do not.

The reasons why we do not are several. These include confirmation biases, groupthink and other cognitive failures; our inability to make sense of complexity; the problem of retrospective coherence; poor or missing incentives to prepare for strategic surprises; and fragmentation of risk (see box story below).

WHY WE FAIL TO ANTICIPATE THE FUTURE

COGNITIVE FAILURES

Decision makers tend to discount *future* risks and contingencies, and place too much weight on *present* costs and benefits. Governments are also prone to *confirmation bias*, which is the tendency to pay attention only to data which is consistent with existing mental models. For example, during the boom years before the current financial crisis, most experts dismissed the risks of a major financial or economic crisis. The few who foresaw an impending crisis – like Nouriel Roubini and Nassim Taleb – were roundly ignored.

Social networks and groupthink are also a source of confirmation bias. Mavericks – whose views do not conform to group opinions – tend to be rejected; they will disappear over time unless a mechanism is set up to protect them. Crises can also break outdated mental models, but they are an expensive way to force recognition of confirmation biases.

What can be done: Well-crafted, challenging scenarios that articulate imaginative yet plausible ways in which the future could evolve, can prompt management to think the unthinkable and consider radical approaches and circumstances.

INABILITY TO MAKE SENSE OF COMPLEXITY

There is a tendency to focus on what can be modelled or extrapolated from today's trends; what is not modelled is discounted or assumed

away. As a result, scenario planners often concentrate on "known unknowns" rather than on "unknown unknowns". But future states of the world can emerge from parallel developments whose interactions are unforeseeable, unforeseen, or unseen, and cannot be predicted from a linear extrapolation of past developments.

Rational, quantitative thinking is easier to deal with than complex, open-ended reasoning. However, the metrics used can fail to reflect reality, and worse, inhibit thinking about underlying complexities in the operating environment.

What can be done: Scenario planning should not be reduced to a simplistic engineering exercise in which driving forces are the inputs, and scenarios, the outputs. Instead, these raw ingredients can interact in bewildering ways to produce unpredictable outcomes and patterns in the eco-system. So in addition to driving forces, look out for potential discontinuities, emerging issues, black swans, wild cards and other strategic surprises.

THE PROBLEM OF RETROSPECTIVE COHERENCE

The current state of affairs always makes sense, but only in hindsight. The current pattern, while logical, is only one of many patterns that could have formed, any one of which would have been equally logical. While the present situation is the result of many decisions taken along the way, retrospective coherence says that even if we were to start again and take the same decisions, there is no certainty we would end up in the same situation.

What can be done: Be aware that the lessons of history are not enough to guide us down the right path into the future. Furthermore, approaches and policies that have worked well in the past may actually prove dysfunctional when applied to the future.

POOR OR MISSING INCENTIVES

Even if individuals and organisations are mentally prepared for a future contingency, they often do not have the incentives to hedge against

it. Hedging is costly, and risks – as the global financial crisis shows – spill across boundaries in ways that make it impossible for a single country to hedge against fully. In the financial crisis, some participants were even incentivised, on a local basis, towards risky behaviour that contributed to the crash. So it was much easier for observers who were not beneficiaries of bank bonuses, such as economist Nouriel Roubini, to contemplate and anticipate a crisis.

The strategic planner often has a hard time challenging the official future, especially when that future is consistent with an organisation's biases and preconceptions. The planner who brings up radical alternatives risks being branded as lacking a sense of reality; he has a real incentive to make scenarios more palatable. But in so doing, he also reduces the impetus for the organisation to confront its uncomfortable futures and prepare for them.

What can be done: Futurist Peter Schwartz once said that the scenario planner should aim to be a court jester – he must be able to say the most ridiculous things and get away with it. The scenario planner is supposed to help us suspend our disbelief.

FRAGMENTATION OF RISK

Hierarchies tend to optimise at the agency level, sometimes at the expense of global optimisation, because information flows most efficiently within vertical silos, rather than horizontally across organisational boundaries. Ministries will tend to have tunnel vision in the way they look at risk. But one arm of government doing something that perfectly matches its "local" performance goals can create a big downside for the rest of the larger system.

What can be done: Take a whole-of-government view and ensure that incentives do not result in perverse behaviour. Avoid the fragmentation of risk by breaking down vertical organisational silos, promoting the horizontal flow of information, and encouraging whole-of-government strategic conversations. ~ Peter Ho

WHAT THE SINGAPORE PUBLIC SERVICE CAN DO

OVER THE YEARS, I have become increasingly convinced that thinking about the future and strategic surprises will remain a messy business. If we try to get precise predictions, we are pursuing the wrong aim. We cannot predict the future. As futurist Peter Schwartz noted, "the objective is not to get a more accurate picture of the world around us".[2] Rather, we should seek to provide input for decision makers to make informed assessments. His colleague from Royal Dutch/Shell, Pierre Wack, added that scenarios should "help change assumptions about how the world works" and "compel people to reorganise their mental models of reality".[3] Good scenarios should facilitate better decisions, not better predictions.

The challenge for us is how we can find a better approach to anticipating strategic surprises. Let me outline five key ideas for our Public Service.

First, we need to acknowledge that we will always face limitations in anticipating strategic surprises. Even in the most forward-looking government, leaders and officials will have their own mental models and cognitive biases, and seek confirmation for them. Being aware that we have biases is already a step forward. When we started scenario planning nearly two decades ago, we were not as sensitised to cognitive biases as we are today. Knowing what we know today, we can take a number of deliberate steps to compensate for our consistency biases.

We should take steps to inject much more real diversity into our strategic conversations. In the United States, the Defense Science Board is commissioned by the Department of Defense to consider strategic issues. Besides bringing experts, academics and professionals to the table, the Board sometimes includes in its discussions people with no defence background at all – artists, actors, musicians. But there is method in this seeming madness. By gathering a diverse group of people, the Board hopes to garner insights that would not be achievable from a team comprising only professionals and experts with similar backgrounds.

In Singapore, we probably have more think-tanks *per capita* than anywhere else in the world. They ought to be tapped more systematically, because they can be a rich source of fresh insights that can better inform policymaking and planning. Conversing with think-tanks, like engaging in public consultation, should be seen as

part of the effort to operate in a complex, inter-connected and non-linear world, in which insight and good ideas are not the monopoly of government.

Networked government does not just mean networking among government agencies. It means networking with individuals and organisations outside government as well, locally and internationally. It is through such ways that we can avoid the trap of groupthink. We should actively organise our strategic conversations to keep an open mind, by encouraging a range of perspectives that do not conform to our own mental models, and by challenging our thinking with contrarian and diverse views. This does not mean we must agree with every view. But we should give each a hearing so as to honestly and objectively test our own ideas.

Second, we should recognise that the cost of responding to some strategic surprises can be just too high politically, especially if governments will be perceived to be allocating an inordinate amount of resources to prepare for eventualities that may never happen. For instance, there is a possibility of the earth being destroyed by a planet-killing asteroid, but this is probably not a risk that we (in Singapore) can meaningfully prepare for, given the prohibitive costs today. We cannot eliminate every risk, but we need to manage them in such a way that strategies and their premiums are not front-loaded.

Third, we have to calibrate strategic thinking processes around the psychological and practical challenges of policy implementation. In addressing these "downstream" issues, methods matter, but psychology matters as well. We will have to harness the relative strengths of the scenario planning and RAHS to mitigate issues of cognitive dissonance and consistency biases.

> Insight and good ideas are not the monopoly of government.

Fourth, it is important to engage and communicate with decision-makers. Their support and active involvement are crucial in achieving better decisions and strategic outcomes. For a message to resonate strongly with decision-makers, the work should be presented in distilled forms, with sufficient detail, using creative expressions and relevant, compelling graphics or visual aids. In addition, complex scenarios and strategies can be broken down into smaller "bite-sized" pieces. These are more easily digested by decision-makers who, in turn, are more likely to recall and apply these insights.

Fifth, we have to recognise that even as we endeavour to avoid being surprised, we should still expect to be surprised. To mitigate this, governments should build some resilience into the system. Among other things, resilience is the ability to address issues with multiple possible trajectories. It is also the ability to adjust to rapid and turbulent change. It is going about our daily business while operating in an environment of near-continuous flux.

Resilience will be an increasingly important driver of competitive advantage in the future. In a world of growing volatility and uncertainty, our approach to policymaking needs to go beyond an emphasis on efficiency, towards building resilience. Indeed, lean systems that are purely focused on only efficiency are unlikely to have sufficient resources to deal with shocks. Of course, this is not an argument for establishing bloated and sluggish bureaucracies. If there is to be "fat", it must be directed to specific purposes.

In this regard, one important idea is to have a small but dedicated group of people to think about the future. The skill-sets needed for long-term policy planning are different from those needed to deal with more immediate volatility and crisis. Both are important. But those charged with thinking about the future should be given the freedom and allocated the bandwidth to focus on this important role without getting bogged down in

ROLES OF THE CENTRE FOR STRATEGIC FUTURES

CHALLENGE CONFORMIST THINKING

- build networks with diverse perspectives within and outside Singapore
- engage local think-tanks and universities, international counterparts and global thought leaders
- conferences on futures-related issues

IDENTIFY EMERGENT RISKS

- communicate emerging issues, wildcards and strategies to decision makers
- in parallel with an integrated WOG Risk Map and Risk Register

CALIBRATE STRATEGIC THINKING PROCESSES

- focus on practical policy development and implementation
- Scenario Planning Plus: integrated framework together with RAHS, WOG Risk Management
- coordinated platform for interagency discussion
- develop new capabilities and a core group of facilitators

CULTIVATE CAPACITIES, INSTINCTS AND HABITS

- mindsets and HR capability for dealing with uncertainty and disruptive shocks
- promote strategic conversations among public servants
- nurture WOG-level strategic thinking and sharing across agency lines on "what if" questions

day-to-day routines. These people will become repositories of patterns that can be used to facilitate decision-making, and especially to prepare for "unknown unknowns". What we need from this small group of people is the capacity to conduct strategic thinking about future possibilities to facilitate more considered decision-making, perhaps even to conduct policy experiments on possible alternative futures, or policymaking by discovery.

> In a world of growing volatility and uncertainty, our approach to policymaking needs to go beyond an emphasis on efficiency, towards building resilience.

A CENTRE FOR STRATEGIC FUTURES

In order to put these principles into operation and strengthen our capacity to think about the future, we have set up a "Centre for Strategic Futures" (CSF) in PSD (see box story on page 64). Over time, together with the Strategic Policy Office and supported by RAHS, the CSF will become the focal point of futures-related work in the Singapore Government. It will work towards promoting whole-of-government thinking on the key strategic issues of the day. It will support the development of capabilities within the Singapore Government in futures methodologies through its core functions.

The Civil Service College will play an important and complementary role to the CSF, by helping civil servants develop the competencies, instincts and habits of mind to tackle uncertainties and manage complexity. This will be done through seminars, programmes and courses on complexity as well as futures thinking and tools, and the documentation of case studies on how the civil service has applied futures work.

While the CSF will play a role in the cultivation of the Government's preparedness for the future, every ministry will also need to build up its individual capability. To facilitate this, we have just established a "Strategic Futures Network", to be made up of Deputy Secretaries from each Ministry. We expect that the Network will play a catalytic role in promoting futures work within the civil service, by expanding the reach of the CSF into the ministries and agencies. The Network will have a key role in establishing a common vocabulary for strategic planning, and nurturing the instincts and habits of strategic whole-of-government thinking about the future.

CONCLUSION

OVERALL, THE CSF will seek to build on the work of scenario planning in facilitating a common, whole-of-government vocabulary for strategic planning. This is important not just to analyse the future, but also to understand the present.

To deal with consistency bias and cognitive dissonance is to nurture in our people the instincts and skills to be sensitive to discontinuities. In an increasingly uncertain and complex environment, it is imperative that we have the courage to open our minds and take bold but pragmatic steps forward. The CSF is an important step in building capability in futures work, and to develop and strengthen interagency collaboration for networked government. The CSF will play a key part in keeping us at the leading edge of governance, enhancing our decision-making capability and the service that we provide to Singaporeans.

ENDNOTES

[1] RAHS incorporates into a computer-based platform a suite of methods and software designed to help analysts detect and investigate emerging strategic threats and opportunities. For more information, see http://www.rahs.org.sg

[2] Dearlove, D., "The Thought Leadership Series Peter Schwartz Thinking the Unthinkable: an interview with Peter Schwartz, scenario planning futurist," *The Business*, September 2002:22-23.

[3] Wack, P., "Scenarios: Uncharted Waters Ahead," *HarvardBusiness Review*, 63 (1985):72-79

EDITOR'S NOTES

This article by Mr. Peter Ho, the former Head of the Singapore Civil Service was originally published in ETHOS Issue 7, January 2010, pg 54-62. The article is based on his speech at the Strategic Perspectives Conference (SPC) on 23 November 2009. His most recent speech at the 2010 SPC provided updates, in particular, on the activities of the Centre of Strategic Futures. For more information, please visit www.cscolllege.gov.sg/ethos.

Risk Assessment and Horizon Scanning Programmes:

The RAHS System

MS. MAGDALENE CHOO

OPERATIONAL IMPETUS FOR EARLY WARNING

The complexity of issues and tempo of activities handled by the Singapore Public Service has increased substantially over the past years, due to an increase in overall scale of activities and inter-connectivity, as well as the interplay of different components exhibiting emergent behaviour. Two examples stand out clearly. One is the declining birth rate in Singapore. To address this, a Government review panel had to look at issues handled by multiple departments, such as employer demands, workplace benefits and employee wages, family cohesion and values, manpower for national defence, and the rising educational status of women. Another example is addressing the threat of Avian Flu spreading to Singapore, which involved the foreign affairs, human health, veterinary health, housing, and transport departments.

Given the complex and multi-domain nature of the issues faced, it is no longer feasible to forecast a future based only on past trends, or to adopt a single-domain strategy when addressing emerging issues. The difficulties faced when adopting a singular future approach are exacerbated by Singapore's unique physical and demographic endowments which are highly vulnerable to potential terror attacks. These include a small country-state that is home to several oil refineries, world-class air and sea transport hub infrastructure, and a heterogeneous population of four main races and several key religions. The Risk Assessment and Horizon Scanning (RAHS) Initiative was thus launched to enable the Public Service to leverage on the vast amounts of data and expertise residing in various agencies. This amalgamation of agencies would result in a better understanding of alternative futures, early warning of arising strategic

threats/opportunities and the ability to engage in anticipatory action to mitigate the impact.

The initiative would involve the utilisation of technology in designing a system that

a. Augments human efforts in the sense-making processes and
b. Enables collaboration and information exchange across various Public Service departments to meet the challenges of understanding and reacting to cross-domain issues.

Through this, the initiative will also ensure optimal allocation of limited Public Service resources, by allowing departments to focus efforts on identified low probability but high impact issues, otherwise termed as wild cards.

The 2 entities which will be supporting this work are the Horizon Scanning Centre (HSC) and the RAHS Experimentation Centre (REC). The HSC will "investigate and recommend, through horizon scanning, case studies or other initiatives, key emerging issues as well as risks or uncertainties across various domains that would have a significant impact on Singapore" while REC will "spearhead technological exploration, experimentation and capability development in support of the Centre for Strategic Futures and the Risk Assessment and Horizon Scanning programme". Together, the HSC and REC will develop the necessary capabilities – concepts and methods, tools and technologies, networks and associations – to perform two key roles: explore emerging issues and investigate complex issues.

SURVEY OF ORGANISATIONS

In a study of various overseas organisations that carry out risk assessment and horizon-scanning functions, it was found that data analytics and scenario planning were the two main methods used in most of the organisations.

The Global Public Health Intelligence Network (GPHIN) was developed for World Health Organisation (WHO) through collaboration with Health Canada in 1996, and functions as a secure Internet-based early warning system that gathers information about potential public health threats on a 24/7 basis. It serves as a web crawler, conducting data mining from various sources, with a focus on infectious diseases and human safety issues. Acting on keywords assigned by Health Canada's Laboratory Centre for Disease control (LCDC) and keywords associated with public, environmental and animal health, it monitors over 10,000 online sources, such as newspapers and biomedical sources.[1]

The *Australia and New Zealand Horizon Scanning Network (ANZHSN)* is an initiative under the Australian Government Department of Health and Ageing (DoHA), that utilises internet scanning and stakeholder consultation to provide

advance notice of significant new and emerging technologies to health departments in Australia and New Zealand, and to exchange information and evaluate the potential impact of emerging technologies on their respective health systems.[2]

The *UK Horizon Scanning Centre*, under the Department of Trade and Industry (DTI), helps identify future issues and trends relevant to the entire public policy spectrum, often employing scenarios and expert consultation in the process. Its aim in such work is to feed into cross-government priority setting and strategy formation. Its work has been used by the Health and Safety Executive to inform scenarios on the future of workplace health and safety.[3]

The traditional Scenario Planning method has also been employed by *Shell International Petroleum Company* to allow the company to anticipate the rise and subsequent fall of oil prices. In the mid-1980s, Shell also created scenarios that focused on the future of the Soviet Union, as that country was a major competitor in the European gas market.[4]

Siemens AG has utilised a form of scenario planning as part of its technological forecasting technique, named "Pictures of the Future". This technique involves selecting a suitable time frame in the future, and generating comprehensive scenarios taking into account various aspects, such as socio-political environments and new customer needs.[5]

The Millennium Project, a global participatory futures research think tank for global issues, has employed scenario planning together with the Delphi participatory method, to produce a large range of scenario sets in various domains such as Demographics and Human Resources, Environmental Change and Biodiversity, Technological Capacity, Governance and Conflict, and International Economics and Wealth.[6]

PRINCIPLES OF THE RAHS SYSTEM

The aim of the RAHS team is to develop a system that comprises a comprehensive suite of methodologies and technologies based on existing work and concepts, with flexibility to cater to future methods and technologies. This system allows the RAHS team to leverage on the advantages of existing methodologies and technologies while acknowledging its constraints.

The two key principles and implementations for the development of the RAHS system are:

a. To leverage on the multiple expertise of individuals. The RAHS system will facilitate collaboration across agencies via linking up various agencies through a common platform, to offer people from different agencies opportunities to communicate and collaborate.

   The inclusion of perspective-sharing facilities enables further knowledge sharing. The analyst is able to

move beyond data sharing to perspective sharing to broaden his perspectives and prevent attention tunnelling when dealing with complexity. Knowledge management expert Dr Dave Snowden has argued for the need for perspectives sharing when operating in the complex domain, in order to gain new views on the situation, rather than rely on entrained patterns from past experience.[7]

b. To focus efforts on analysis. Technologies will be available to augment their work in performing searches, analysing the search results and creating models.

Firstly, the RAHS software will reduce the amount of time spent on searches. It consists of a range of analytical tools, which aid the analyst in reducing the amount of reading time required, as well as software to automate the running of pre-determined workflows.

Secondly, the analyst can use the RAHS software to create models for sense-making and monitoring. According to the Naturalistic Decision Making framework developed by Dr. Gary Klein[8], experts rely on mental models and pattern matching against these models to discern subtle clues and choose the correct path of actions when dealing with complex situations with high levels of uncertainty. This hypothesis was further substantiated and popularised by subsequent publications from Dr. Klein[9], as well as by Malcolm Gladwell[10]. Along this line, the RAHS System explores the use of various models as different means of data structuring, to help the analyst better make sense of incoming data and monitor the situation.

SYSTEM OVERVIEW: METHODOLOGIES & TECHNOLOGIES

THERE ARE 3 major capability blocks in the RAHS Software. The research and analysis tools allow analysts to closely examine signals collected from environmental scanning. The perspective-sharing tools allow analysts to offer insights on pieces of information they receive, and for these perspectives to be analysed for convergence and divergence, and for possible outliers or even wild cards. The scenario building tools allow analysts to build system maps and ranking models, and to examine various scenario and strategy options.

RESEARCH AND ANALYSIS

THE RAHS SOFTWARE empowers analysts with a suite of tools, to help them process large amount of data, which can either be unstructured text obtained from the

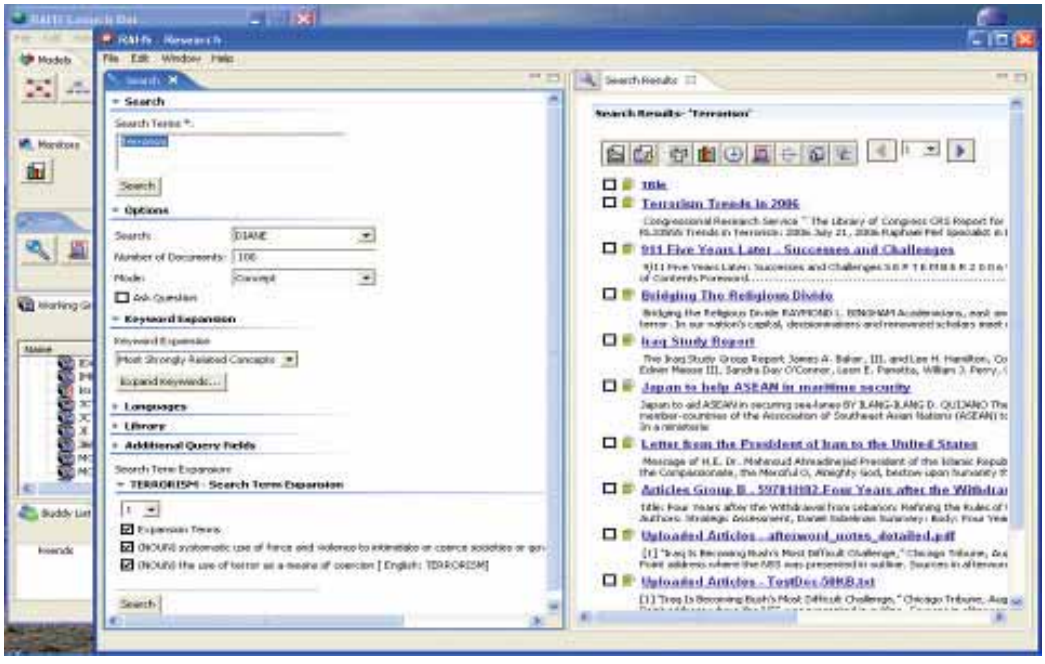


Figure 1: Screen Shot of the Advanced Search Tool

Internet or reports uploaded by the analysts. The system gives analysts the flexibility to apply these analytical tools in any order, in support of the analytic process. The following section describes various analytical tools:

Advanced Search Tool

The RAHS software allows analysts to search for articles within its repository *(refer to Figure 1)*. The Advanced Search tool provides powerful features for fine-tuning text searches. Analysts can select different search modes, specific libraries and filter search through fielded queries.

Summary Tool

A common problem faced by analysts today, is having to read through a collection of articles, after which realising that only a handful are relevant to the topic of research. The RAHS multiple document summariser will thus be useful in reducing the amount of reading required, by picking up key sentences that best summarise a single article or a collection of articles *(refer to Figure 2)*.

Entity Analysis Tool

An entity is an object that can be a human, a location, an organisation, dates and times, monetary amount or percentage; Entity Analysis thus is the process of extracting such objects from raw data. This is based on automatic word alignment of speech recognition output, through natural language processing of the

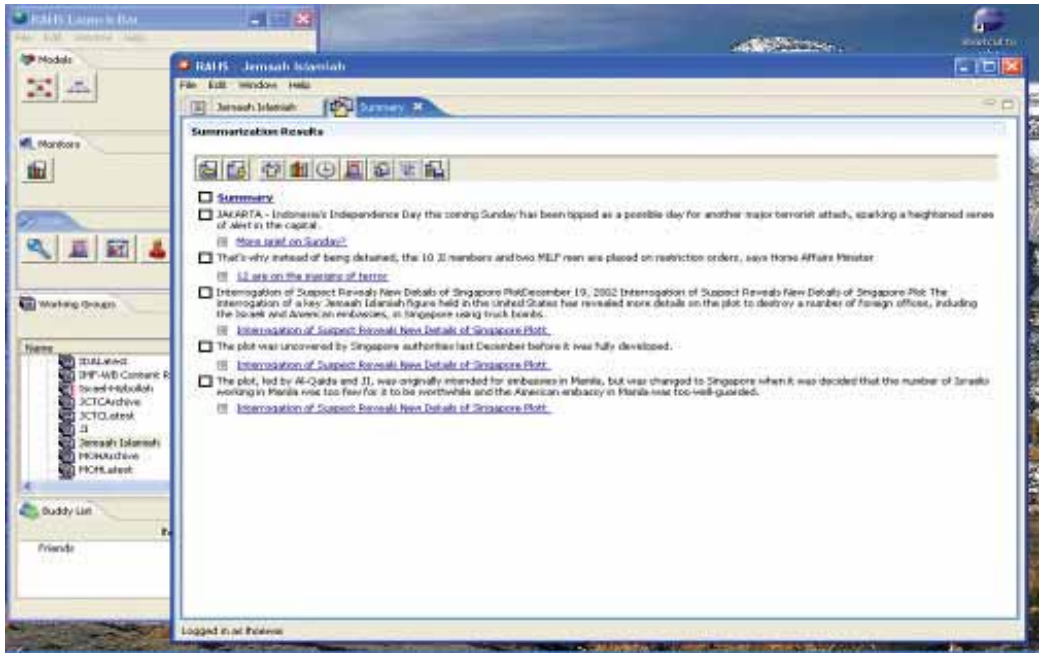


Figure 2: Screen Shot of the Summary Tool

English grammar and language. The RAHS system includes an entity analysis tool, as well as other variants *(also see Figures 3 and 4)*. The variations are:

a. The Temporal Analysis Tool shows references to entities extracted from the entity analysis tool over time.
b. The Cross-sectional Analysis Tool shows the other entities that are mentioned in the same article as a particular entity of interest.
c. The Keyword Analysis Tool extracts 'terms' or 'phrases' pre-determined by analysts and counts the occurrences of these 'keywords' in a set of documents.

Timeline Analysis Tool

TIMELINE ANALYSIS IS the extraction of events (with a best estimate of when these events had occurred) from a set of articles, using a set of analyst-supplied query terms. The Timeline Analysis tool in the RAHS system performs this function, and also assigns ranking scores to these events, based on how significant these events are to the query terms *(refer to Figure 5)*.

Clustering Tool

CLUSTERING IS AN analytic process, where a collection of articles are arranged such that similar articles are grouped together *(refer to Figure 6)*. This process,

which can be done automatically or manually, can be used to:

a. Identify hidden relationships between groups of objects which arise from a search result, to help the analyst better refine his/her search query.

b. Ease the process of browsing, to find similar or related

Figure 3: Screen Shot of the (clockwise from left) Entity Analysis Tool (with pie chart illustration), Temporal Analysis Tool, and Cross-sectional Analysis Tool

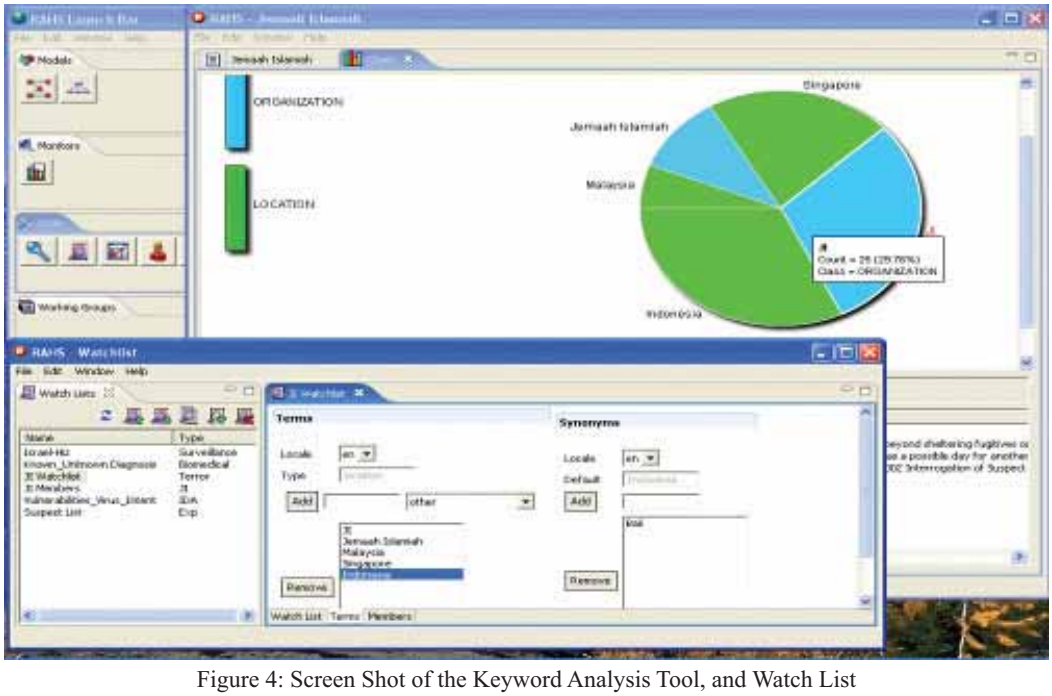


Figure 4: Screen Shot of the Keyword Analysis Tool, and Watch List

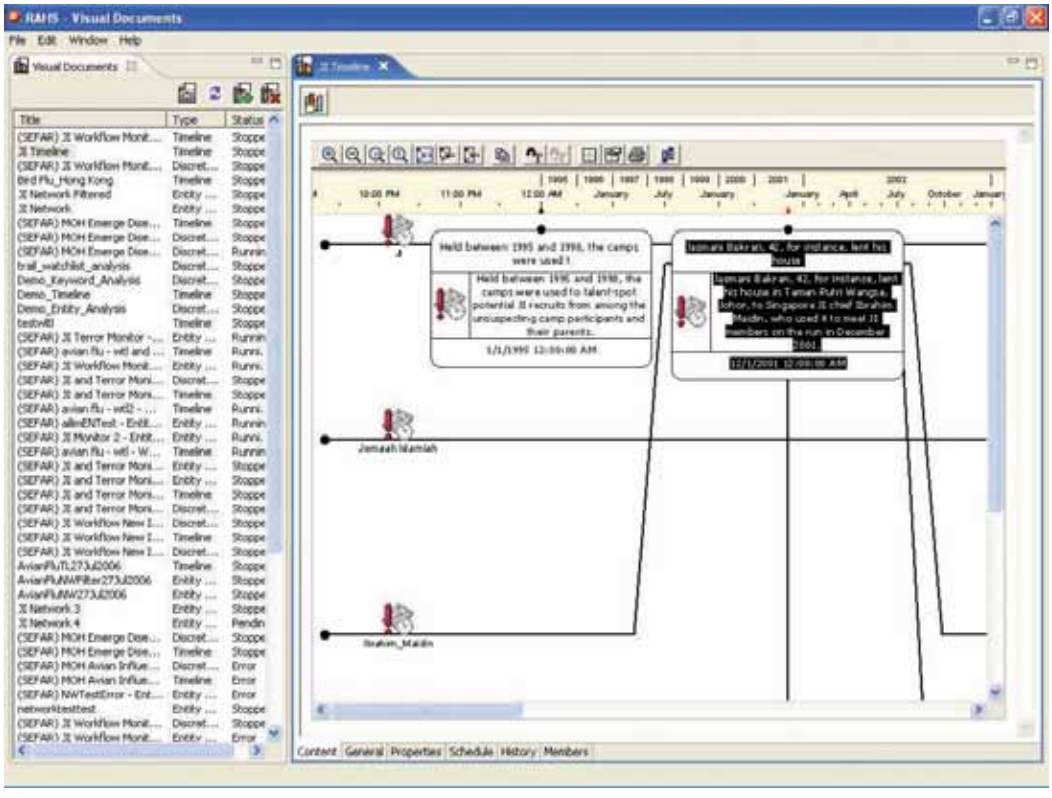


Figure 5: Screen Shot of the Timeline Analysis Tool

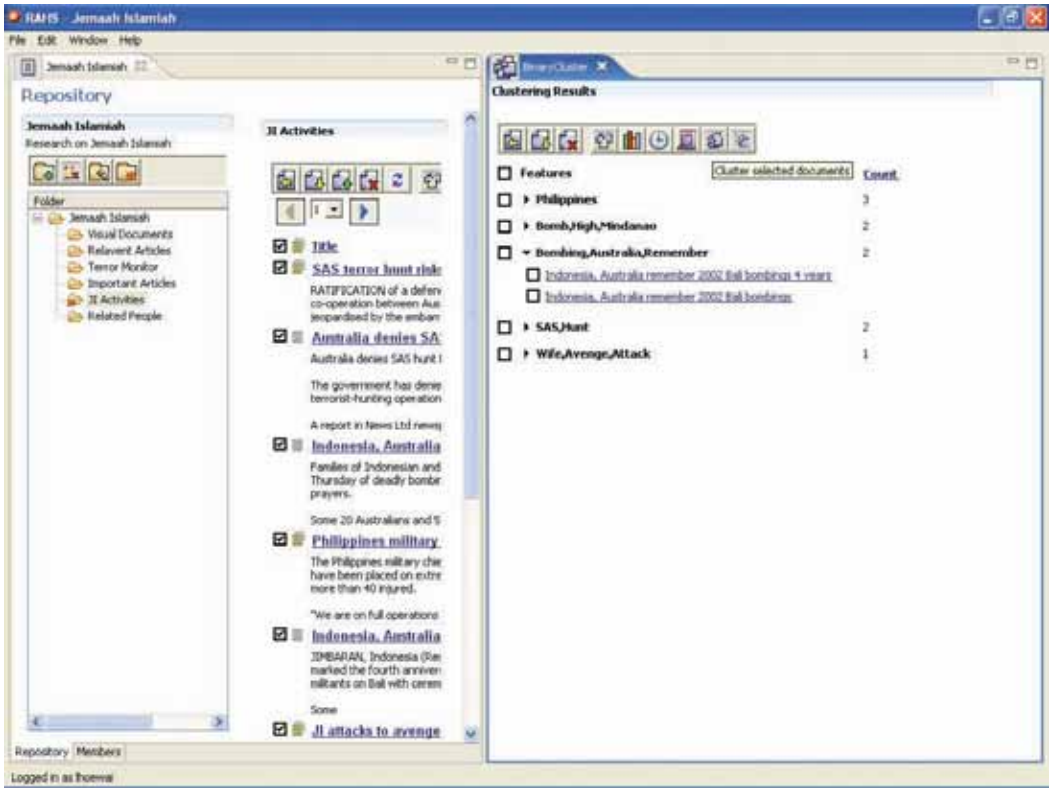


Figure 6: Screen Shot of the Clustering/Duplicate Document Detection Tools

information from a search result, helping the analyst to obtain information.

c. Find unique topics within a collection of articles. The unique topics might draw the attention of the analyst to new trends or patterns, which have not yet been mentioned in other articles.

In addition to these tools, others to provide (a) perspective sharing and (b) data organising capabilities are also available in the RAHS software.

Automated workflow

To speed up routine tasks, the RAHS software has the ability to automate the analyst's work process of performing searches on the various data sources, moving the articles into project folders, and performing of entity, timeline and network analysis on the consolidated articles, resulting in various visualisations *(Figure 7)*. Should the user analyst discover interesting information from the analytical visualisations, he/she can then choose to perform further analysis on the system.

PERSPECTIVE SHARING

The RAHS software incorporates the ability to elicit and analyse perspectives from various agencies/stakeholders. The analyst can provide his/her perspective of a data item by meta-tagging the articles. The meta-tag not only facilitates easy retrieval of individual data, but also helps reveal outliers when meta-tags of various data are viewed together.

In addition, the meta-tags of the other analysts working on the same project will provide alternative perspectives to the first analyst, thus avoiding the danger of being blind-sided through premature convergence. Two tools to enable perspective sharing, namely the Indexing and Perspective Visualisation Tools, will be elaborated upon.

Indexing Tool

The RAHS system provides an indexing software to allow analysts to meta-tag articles *(Figure 8)*. Four types of meta-tags are provided: Filters, Questions, Comments and Keywords. Filters are abstract, stylised and broad concepts that represent a specific research problem. There are two main types of filters: emergent filters and analytical filters. Emergent filters consist of Archetypes, Values and Themes (AVT), and analytical filters consist of opposing negatives or opposing positives. The analyst can select from a range of Filters, and specify the extent to which each Filter best describe a piece of data, by selecting from a range of values in each Filter. Questions are concrete, factual and detailed. Each Question has a set of

predefined options for the analyst to decide which option best describes the data. Filters and questions can be used in relation to each other such that the questions constrain the filters.

Comment and Keywords are freeform meta-tags that are analyst-specific. Comment meta-tags allow the analyst to enter freeform text, while Keyword meta-tags allow entry of multiple analyst-specific words or sentences relating to a particular piece of data.

Perspective Visualisation Tools

The meta-tags entered are representations of the analyst perspective, and the RAHS software provides a set of visualisation tools specially designed to help analysis of such perspectives and accompanying data. The seven types of visualisation tools *(Figure 9-15)* – Glance, Browse, Compare, Range, Distribute, Cluster and Graph – provide different ways of looking at the data.

Patterns and models are meant to be the primary form of analysis with the statistics and data as supporting evidences. The visualisation of patterns aims to enable the user to interact with the data and adopt an outsider's viewpoint in analysing the meaning of the data. Since the filters and questions represent the hypotheses in the research, the researcher/person analysing the data should have an idea of the relationships between the factors. Thus, interesting patterns would be combinations of factors that the knowledgeable researcher expected and was confirmed by the research and combinations of the factors that he did not expect. Prioritisation for further analysis of the factors would depend on the expert judgment of the knowledgeable researcher. Further analysis would require the same research process with more refined filters and questions. This follows in the assumption that humans are pattern processors and that insights gained from the information need to come from the analyst who have a general sense of the field.

MODEL CREATION AND MONITORING

Data organising capabilities to enable the analyst to build models and enable collaborative modelling efforts are incorporated into the RAHS software, thus allowing analysts to connect across silos and challenge previous thinking assumptions. Capabilities for model monitoring will also be provided, to enable matching of models with incoming data streams, and to allow the human team to explore the interpretations and implications of these data.

The RAHS system currently focuses on organising information into two model classes: expert-based modelling techniques and ground

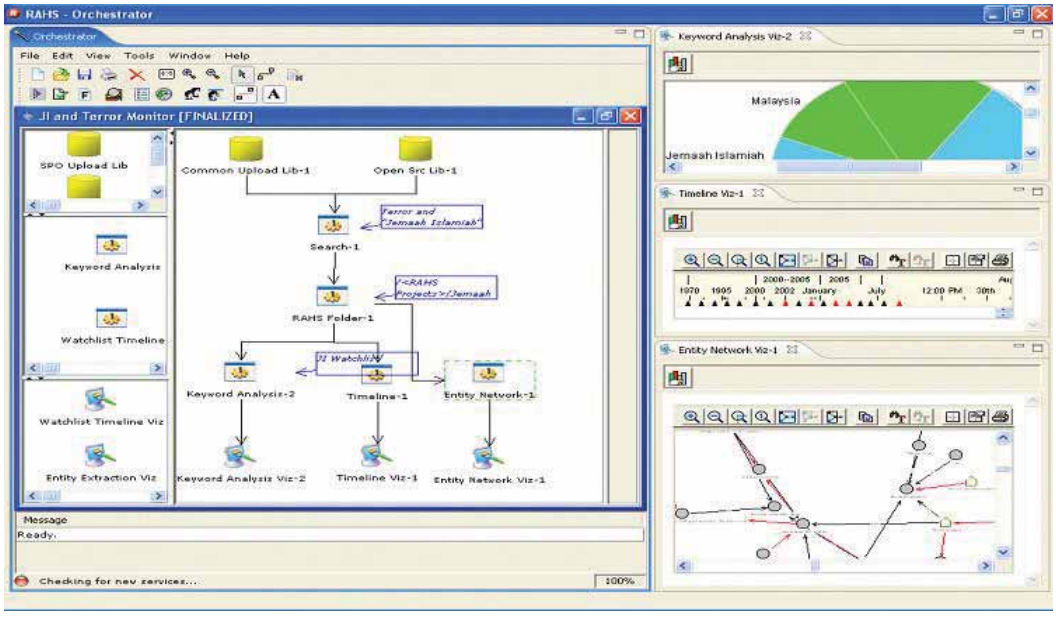


Figure 7: Example of automated workflow

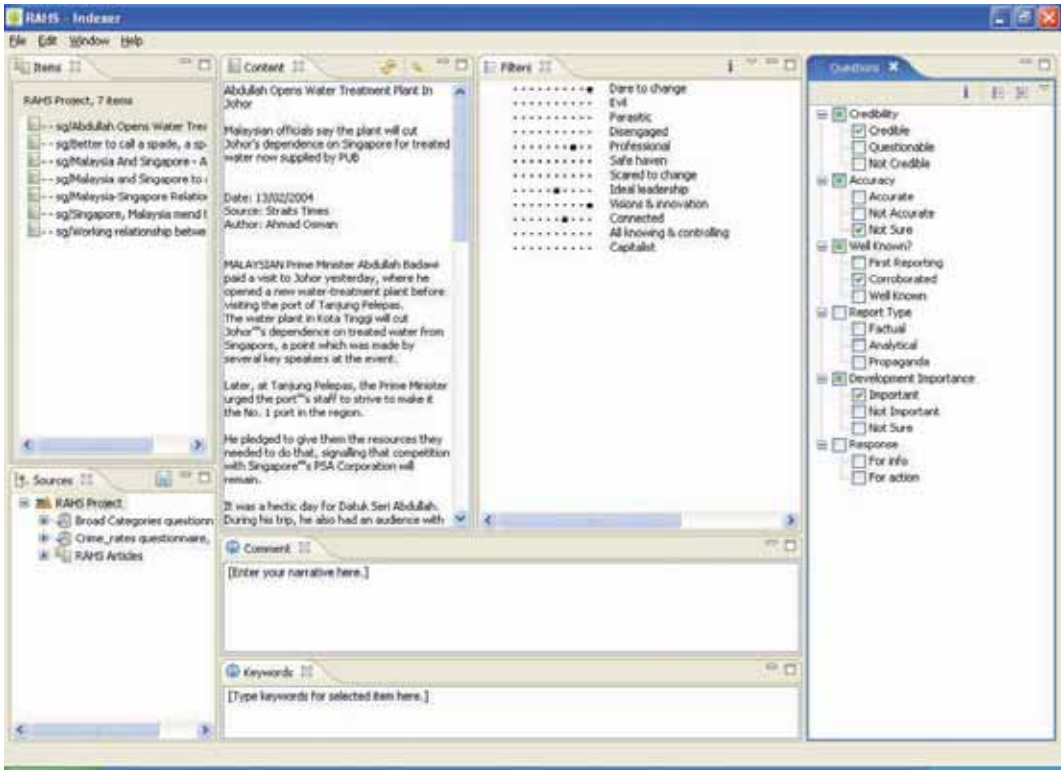


Figure 8: Screen Shot of the Indexer Tool

up, information-driven models. The Scenario Builder tool was developed to facilitate the analyst's work in building expert-based models while the Perspective-based Pattern Detection (PPD) suite was designed to enhance the understanding of incoming information.

Scenario Builder tools

The Scenario Builder tool in the RAHS software enables the analyst to create a system model (referred to as a System Map) based on Systems Thinking. This depicts the analyst's understanding of the factors/components of the system or situation being studied, as well as the relationships between these factors.

The System Map helps the analysts clarify their understanding of the eco-system of events and people, and serves as a basis for in-depth discussion and sense-making. A set of supportive tools, such as that to help find out the most influenced and most influential factors, are also provided to help derive more insights from the System Map. A sample System Map and its Influenced/Influential Map is illustrated at Figure 16.

Having built the System Map, the analyst can further input the states for each factor, along with the pair-wise consistency between each pair of states of two different factors. After the options for the factors and the consistencies are provided, the RAHS system will then be able to carry out Morphological Analysis[11], and generate a spread of all possible scenarios or strategies *(Figure 17)*.

PPD modelling tools

The second group of models that can be built is that of the PPD models. These consist of the Cynefin framework and the future backwards model. They are developed by building on concepts from the exemplars of an incident or event. This is similar to defining a category of people, for example, exemplars of terrorists could be Osama bin Laden and Azahari Hussein.

The Cynefin framework is a sense-making model developed by Cognitive edge. It consists of five domains: known, knowable, complex, chaos and disorder. The first domain represents cause and effect relationships that are not open to dispute, and actions can follow standard operating procedures. The second domain is knowable. It consists of information that is not fully known but can be known given enough time and resources. The actions associated with this domain are research and planning. The third domain represents complex information space where information either does not follow a stable trend, or that the factors that make up the trend are not obvious to inspection. Relationships and trends

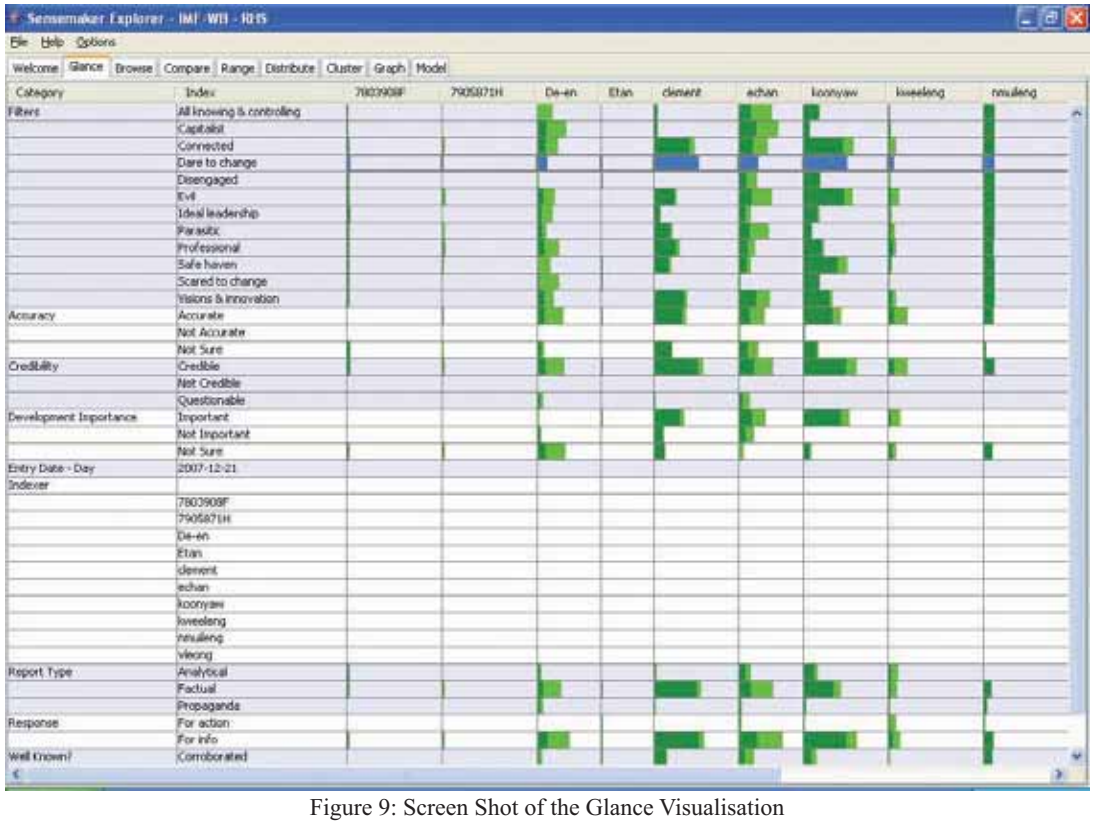


Figure 9: Screen Shot of the Glance Visualisation

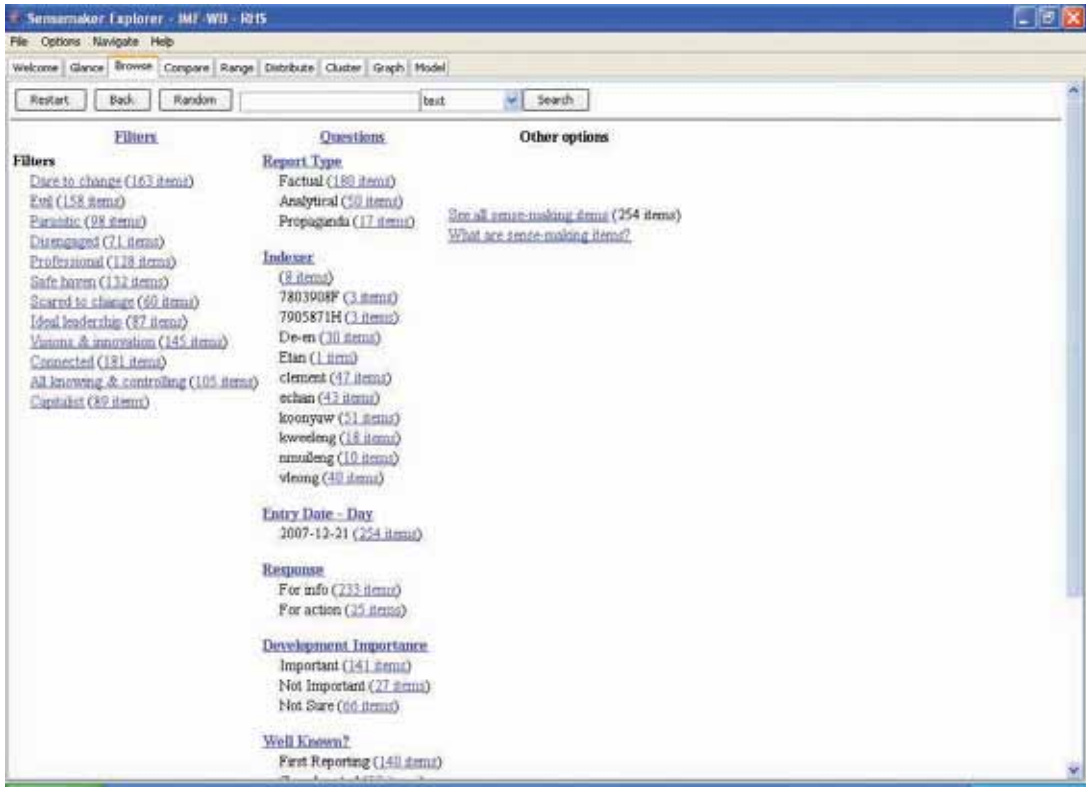


Figure 10: Screen Shot of the Browse Visualisation

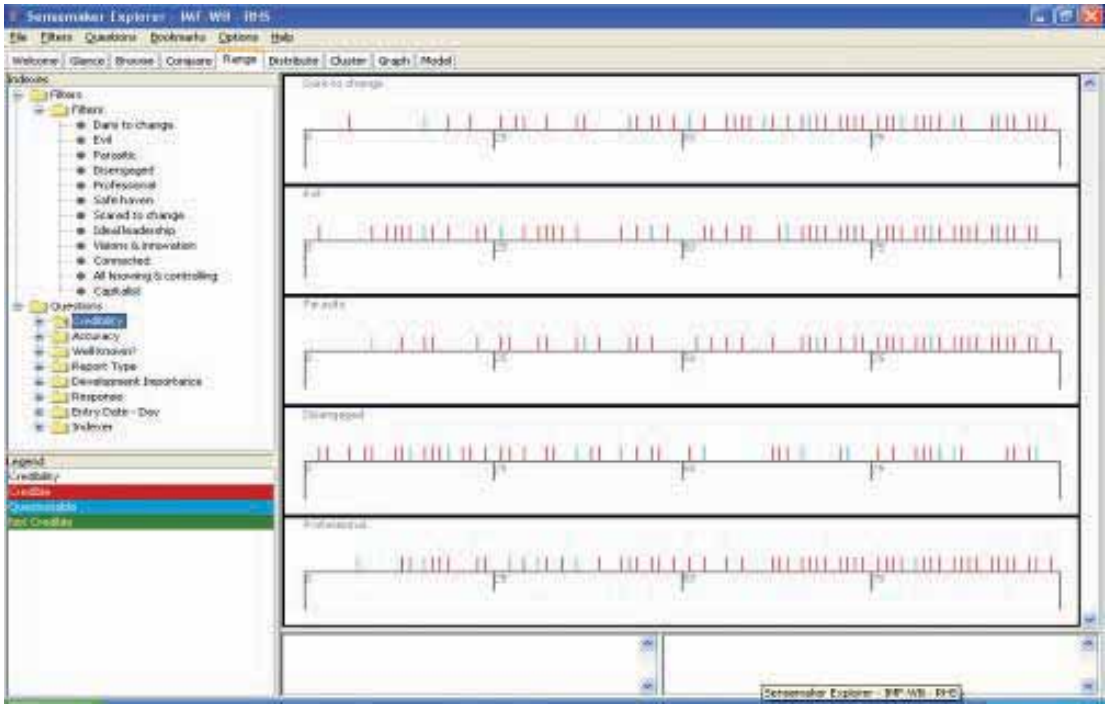


Figure 11: Screen Shot of the Compare Visualisation

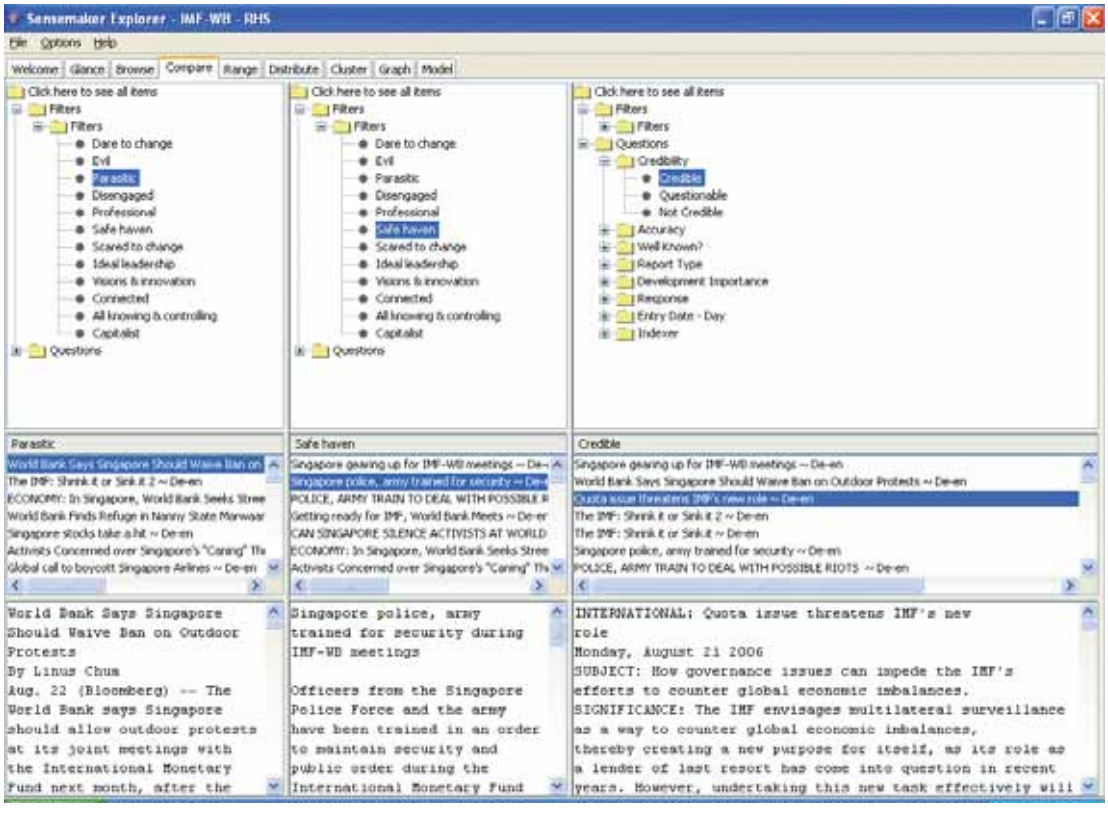


Figure 12: Screen Shot of the Range Visualisation

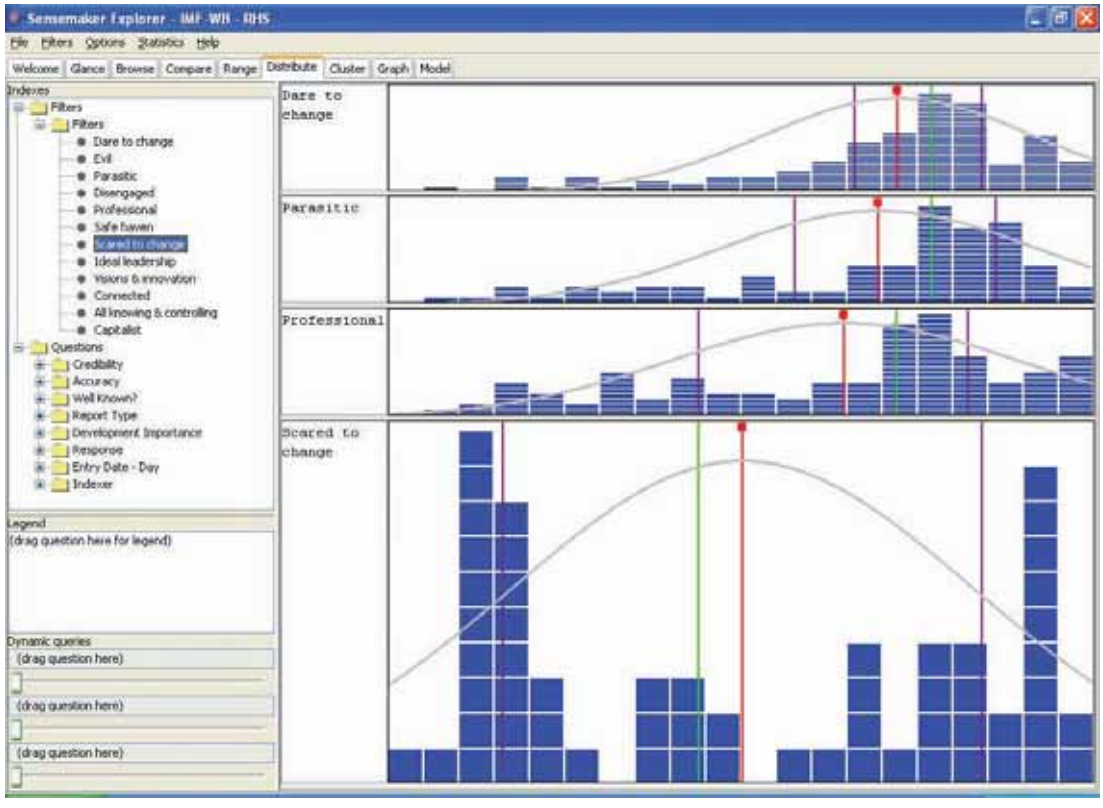


Figure 13: Screen Shot of the Distribute Visualisation

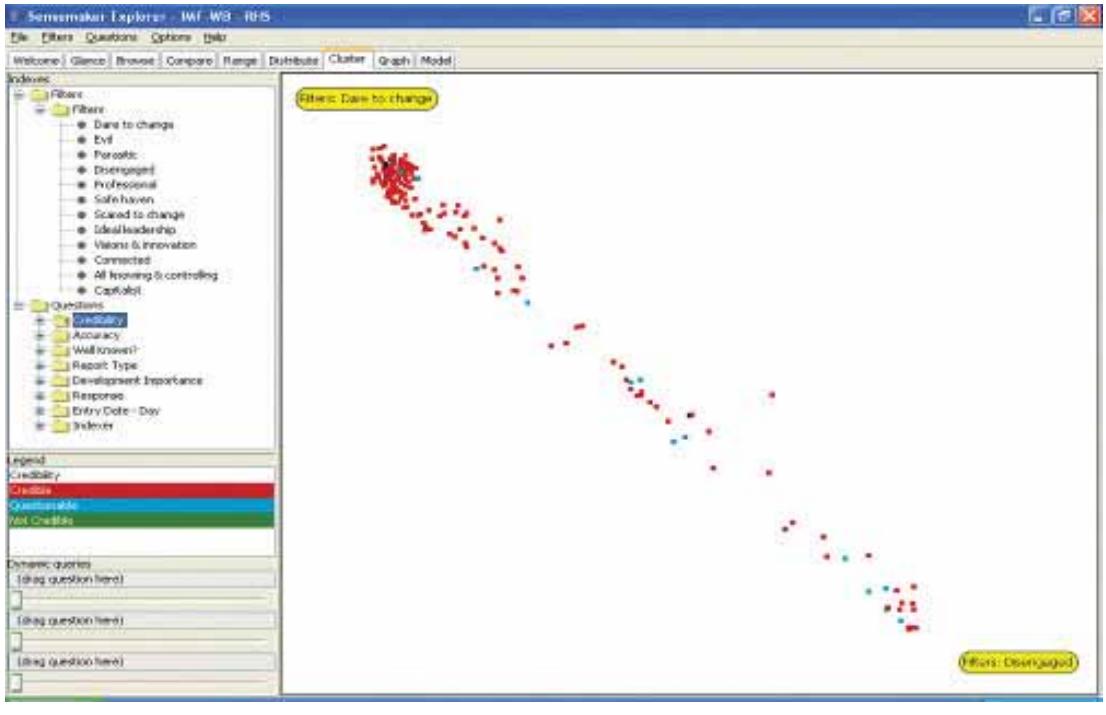


Figure 14: Screen Shot of the Cluster Visualisation

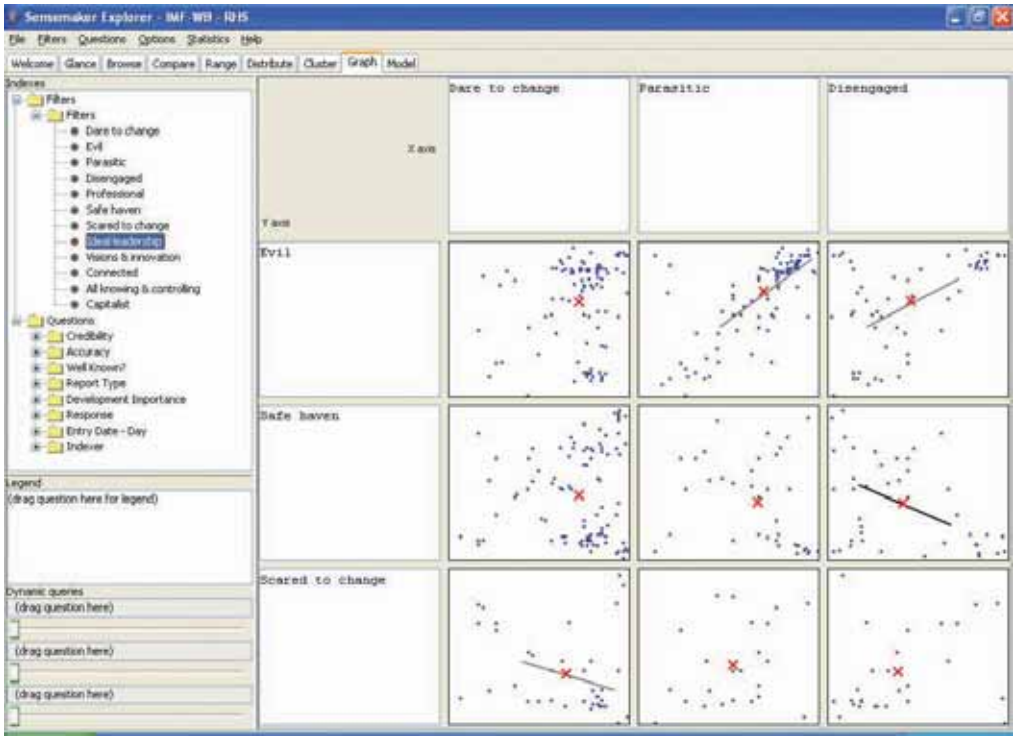


Figure 15: Screen Shot of the Graph Visualisation

cannot be perceived in the chaos domain, and innovative actions need to be taken to rectify the issues. In the central domain of disorder, the issues and information do not fit well into any of the previously described domains, instead, they have a combination of the elements of the domains.

In the RAHS software, the Cynefin framework facility enables the user to attach evidence in the form of articles on the framework *(Figure 18)*.

Development of the Future-Backwards model encourages the analyst to consider the steps that were taken to arrive at the current state of affairs, steps that can be taken to arrive at the impossibly good future and the impossibly bad future. The electronic version of the Future-Backwards model in RAHS enables an electronic copy of the steps to be listed and the evidence to support the steps to be stated and stored *(Figure 19)*.

Monitoring Tool

To monitor the situation, the analyst can create filters for each of the factors, so that incoming data streams can be extracted and matched to each factor. The analyst can then take note if the incoming data implies a situation different from the model currently depicted by the System Map and its associated

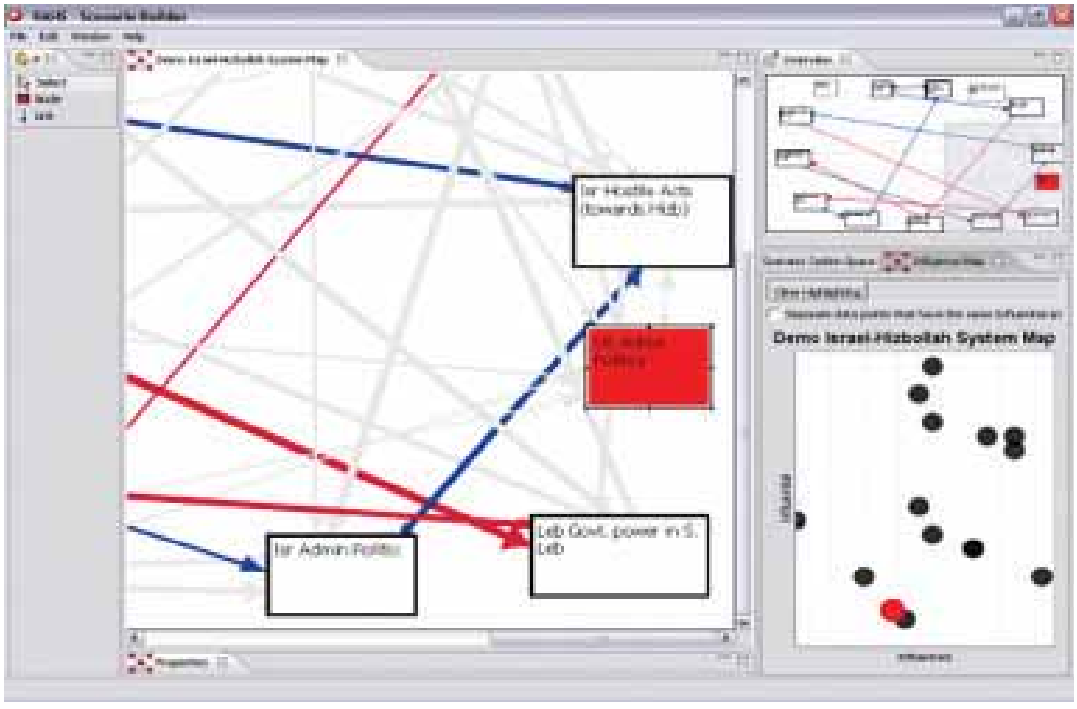


Figure 16: A System Map on the left, with its Influenced/Influential Map in the lower right.

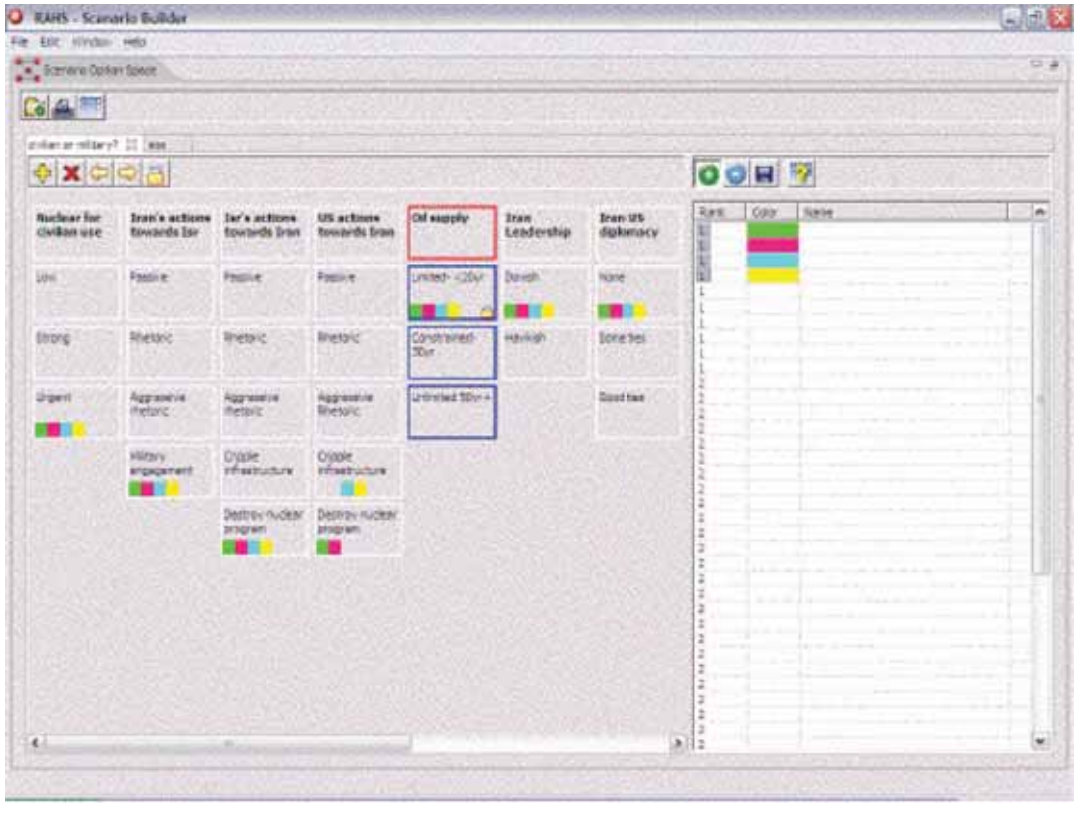


Figure 17: A Morphological Analysis with different scenarios highlighted

consistencies, and revise his/her existing model. The data input can also help the analyst to monitor development of the situation, and to narrow down to the possible scenarios that are likely to unfold in the near future.

FUTURE DEVELOPMENTS

BUILDING ON THE strength of scenario planning, HSC has partnered the Strategic Policy Office (SPO) to develop a Scenario Planning+ (SP+) methodology which integrates systems thinking and morphological analysis. The RAHS tools allow for component processes in scenario planning to be carried out on a more complex scale. The SP+ tool kit therefore offers analysts a range of concepts & methods to choose from. Specific combinations of concepts & methods will be recommended once a problem has been identified and the problem space has been defined.

The HSC will also be developing a primer to help transmit the necessary processes and skills. There is quite a fair bit of conceptual work that needs to be done. Emerging Issues need to be understood in relation to the Risk Management cycle, and in association with Discontinuities and Global Shifts. We need to better understand how devil's advocacy, red teaming and alternative analysis can h elp the process. And we need to understand the growing lexicon of '*black swans*'[12] and '*dragon kings*'[13].

The RAHS Experimentation Centre works closely with HSC to better understand their needs and introduce cutting-edge technologies to reduce the cognitive burden of analysts and improve their effectiveness. Some areas of exploration include trend analysis, sentiment analysis, information fusion and interdependency modelling. REC also manages the development of RAHS 2.0, the next generation of the system, which will have a broader range of sophisticated capabilities to enable future works.

CONCLUSION

THE RAHS SYSTEM is a network of people, data and tools with a wide range of methodologies that can cater to different problems and situations. Its open architecture enables it to evolve continuously, to connect with new agencies and incorporate new concepts and technologies. This is done with the aim of leveraging on a wider source of people, expertise and data, both locally and internationally. Thus working towards enhancing Singapore's early warning capabilities with regards to threats/opportunities affecting our national interest.

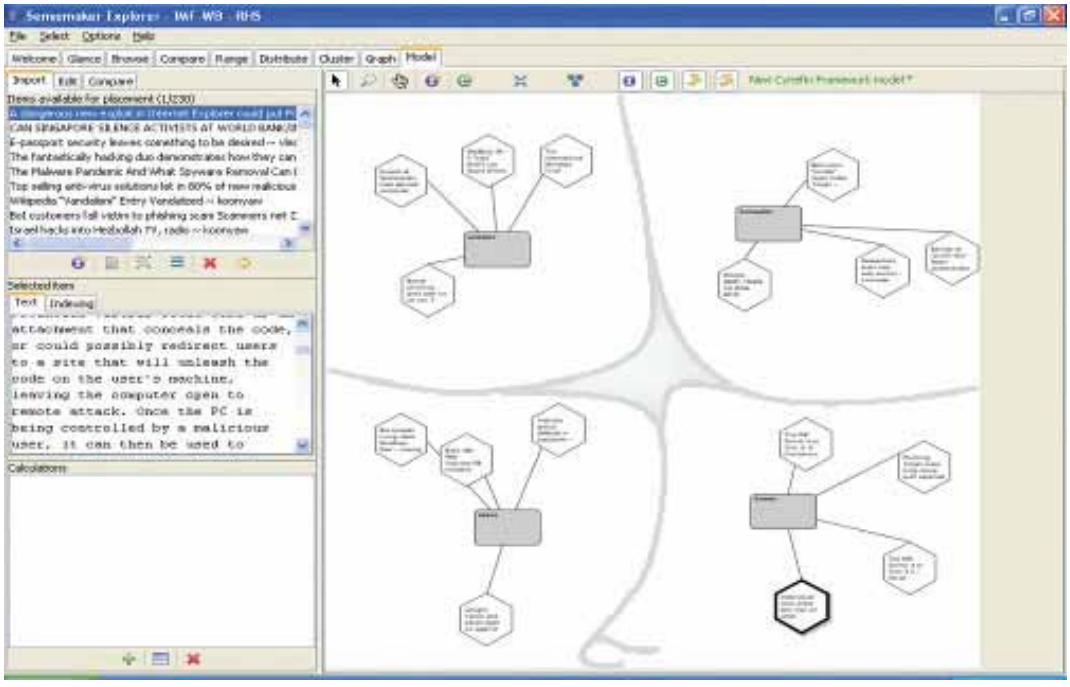


Figure 18: The Cynefin framework

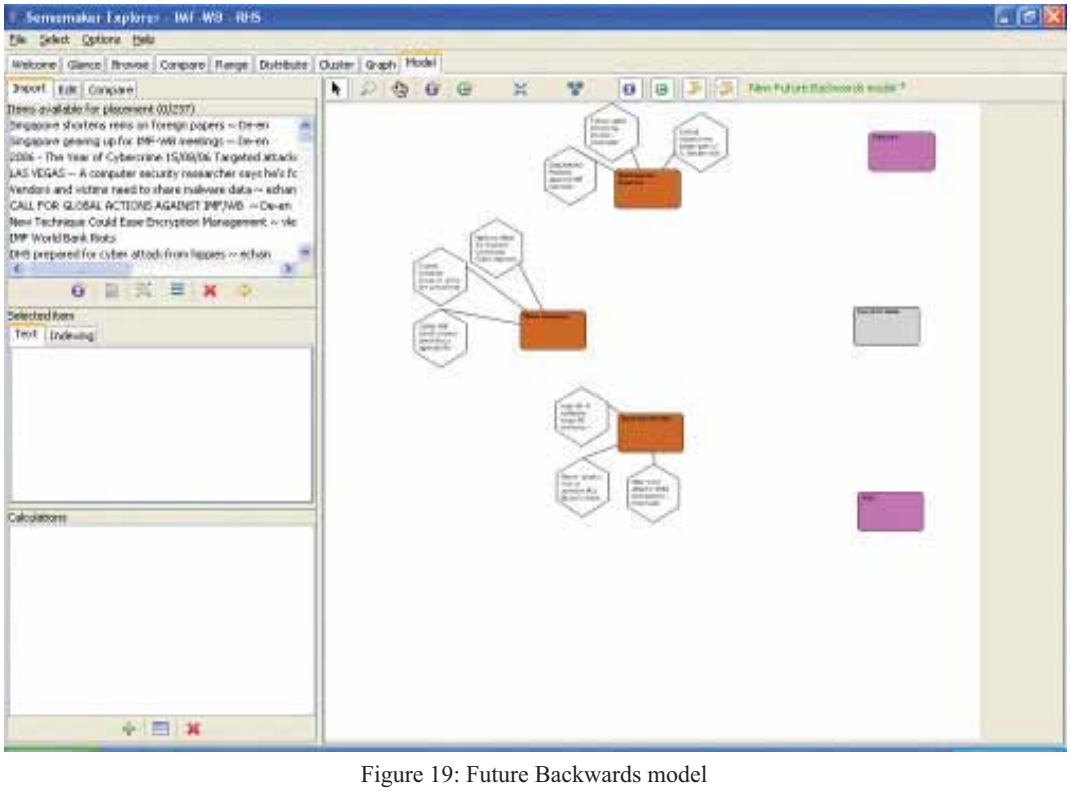


Figure 19: Future Backwards model

REFERENCES

1. More background at the Carleton University website at: http://www.carleton.ca/jmc/cnews/12031999/f4.htm
2. Details at the DoHA website at: http://www.horizonscanning.gov.au/
3. More info at the DTI website at: http://www.gnn.gov.uk/environment/fullDetail.asp?ReleaseID=251912&NewsAreaID=2&NavigatedFromDepartment=False
4. Details in Chp 13 "Scenarios", Futures Research Methodology CD-ROM v2.0 on, by the Millennium Project.
5. Details at Siemens' website: http://www.siemens.com/index.jsp?sdc_p=ft4mls3u20o1156534n1156534i1168864pFEcz2&sdc_sid=21842775797&
6. Details at the AC/UNU Millennium Project website: http://www.acunu.org/millennium/environscen.html
7. The new dynamics of strategy: Sense-making in a complex and complicated world
8. Sources of Power: How People Make Decisions
9. The Power of Intuition: How to Use Your Gut Feelings to Make Better Decisions at Work
10. Blink: The Power of Thinking Without Thinking
11. Ritchey, T. General Morphological Analysis: A general method for non-quantified modeling. http://www.swemorph.com/pdf/gma.pdf
12. The Black Swan Theory is used by Nassim Nicholas Taleb in his book 'The Black Swan' to explain the existence and occurrence of high-impact, hard-to-predict and rare events that are beyond the realm of normal expectations.
13. It was first used by Didier Sornette in his article "Dragon-Kings, Black Swans and the Prediction of Crises", Swiss Finance Institute Research Paper No. 09-36, September 9, 2009

EDITOR'S NOTES

Ms Magdalene Choo is an Assistant Director at the Horizon Scanning Centre (HSC). The HSC is located within the National Security Coordination Secretariat (NSCS). HSC explores and investigates, through horizon scanning, case studies or other initiatives, key emerging issues as well as risks or uncertainties across various domains that would have significant impact on Singapore. Scenario Planning has been central to the Singapore Government's ability to plan and prepare for a range of possible futures. The Risk Assessment and Horizon Scanning (RAHS) programme was launched in 2004 to explore methods, tools and techniques that could complement scenario planning.

Bioterrorism *in the* mail:

An innovative USPIS response to a new challenge

MR. OSCAR VILLANUEVA

As the law enforcement and security arm of the United States Postal Service (USPS) and one of the oldest federal law enforcement agencies in the country, the United States Postal Inspection Service (USPIS) has the jurisdiction to investigate any illegal use of the mail within the United States. United States Postal Inspectors trace their lineage to the 1700s when a similar position was created under the British postal system which was operating in the American colonies. During these colonial times, Postal Inspectors began a long and successful history of investigating postal crimes to include the mailing of injurious articles containing chemical, biological, radiological, and explosive threats, and bringing the responsible criminals to justice.

Package bombs, poisons, and other weapons are occasionally and illegally sent through the mails in an attempt to injure or kill the recipient. While these worldwide incidents are rare and the reasons varied, often resulting from business disagreements, revenge, or a lover's quarrel, the end result is the same – severe injury or death. The sophistication of these injurious items has evolved over the years not to mention, also improving on their effectiveness of causing harm and injury to the recipient. In the United States (US) this evolution has required an ongoing corresponding development of new training and methods used by US Postal Inspectors to effectively and decisively address this threat.

ANTHRAX IN THE MAIL

A new age of terrorism came upon us following the September 11 attack of the World Trade Center in New York. This significant terrorist incident brought with it a new challenge and a renewed sense of urgency to the law enforcement and security

communities in the US and abroad. In the case of the USPIS, a new challenge was created with the unprecedented Anthrax mailings in late 2001. The use of the mails for bioterrorism caused a new threat paradigm requiring a prompt solution and the creation of new and robust investigative and prevention programmes.

On 18 Sep 2001, only a few days after the September 11 attacks, letters containing anthrax spores were mailed to several news media offices and two U.S. Senators, killing five people and infecting 17 others. The USPS implemented unprecedented precautions and prevention protocols in the aftermath of this incident. These prevention efforts were very costly requiring that the over 250 large mail processing facilities be equipped with sophisticated detection equipment to screen for biological threats. This high level of preparedness provided a level of protection required to allow the seamless operation of the postal system.

"The use of the mails for bioterrorism caused a new threat paradigm requiring a prompt solution and the creation of new and robust investigative and prevention programmes."

The mailing of letters containing Anthrax (bacillus anthraces) had a tremendous impact on the USPS and Postal Inspectors. For the first time, the mail had been used to successfully convey a weapon of mass destruction. The results of the attacks were devastating for the victims and created, for awhile, a fear of the mail. The potential impact to the USPS was significant. Fortunately, those fears subsided as the USPS and Postal Inspectors took action and people realised that mail was and continues to be safe.

The strategic development of a solution to this problem was initiated as the USPS developed ways, many very technical in nature, to make sure every reasonable precaution was in place to deter and detect another attack. The technology necessary for such prevention and detection did not exist in a form that could be quickly applied to mail processing. A team of scientists, biological weapons experts, mail processing engineers, and Postal Inspectors evaluated existing technology that could potentially be used to detect harmful substances contained in mail and, in a surprisingly short time, the Biohazard Detection System (BDS) was developed, built, and deployed in every USPS mail processing center. The initial cost and associated operating expenses are enormous costing more than one billion US dollars, but the resulting system has proven to be highly effective, ensuring that the mail, Postal Service employees and the public are

protected. The incredible investment to implement BDS is just one example of the USPS commitment to ensuring the integrity of its service and maintaining the trust associated with the mail.

DEVELOPMENT OF A SECURITY AND LAW ENFORCEMENT RESPONSE TO BIOLOGICAL THREATS

For many years, the USPIS has responded to reports of suspicious mail articles. In fact, Postal Inspectors were integral to the initial development of the first portable x-ray units now considered a basic tool of bomb technicians worldwide. As the USPS and USPIS began to develop plans to address the growing threat of chemical, biological and radiological weapons beyond the implementation of the BDS system, they were able to draw on the hundreds of already trained Postal Inspectors and their portable x-ray units strategically located across the United States. Additional training and equipment was required to effectively address this new threat. This required an expanded use of existing processes and the establishment of protocols necessary to deploy new tools and training. The technology part of this deployment was no small task as interested biohazard equipment vendors and manufacturers were making many questionable and unsubstantiated claims and promises in response to the panic created by the specter of an additional biological attack.

While an appropriate Postal Inspector incident response protocol was in place, the challenge was finding the right combination of equipment, training and protocols to ensure proper protection of USPS employees, the mail, and the American public, while preventing unnecessary disruptions of postal operations. This task was exacerbated by existing municipal fire department protocols in the United States. These first responders commonly provide hazardous materials response using field testing processes and equipment without proven records of accuracy, and with an unacceptable numbers of false positives. The lack of uniformity compromised the USPIS's ability to ensure that all areas of the USPS were handled with comparable levels of protection and that unnecessary operational disruptions were minimised.

In the mail paranoia following the Anthrax mailings, responses to mail processing centers by municipal fire departments across the country were resulting in unnecessarily shutting down operations due to unreliable false-positive field test results, with many substances tested eventually being confirmed as sugar, chalk and other similarly harmless substances. Worse yet, employees and the public sometimes had to wait 24 hours or longer periods of time before receiving confirmation that they

had not been exposed to hazardous substances. These conditions were clearly unacceptable to the USPS and the American public. The unnecessary evacuations, particularly in large facilities with hundreds or even thousands of employees resulted in much disruption to employees, customers and operations, and frequently delayed mail delivery.

After much evaluation and consultation with experts in chemical, biological, and radiological weapons, a tiered response system was adopted that uses a combination of training, field screening equipment, and clear criteria for testing on site, while seeking accurate and timely laboratory confirmation of field findings. In order to implement this new response system and deploy it throughout the country the USPIS provided highly technical training, including HAZWOPER, to over 300 Postal Inspectors, and engaged in the procurement of a fleet of specially designed response vehicles containing the latest in chemical, biological, radioactive, and nuclear hazard identification tools. This investment in training and equipment places the USPIS far ahead of many other law enforcement and public service agency in the United States in its ability to efficiently respond to threats of this type.

While the equipment and training was and continues to be very costly, the return on this investment has been significant, dramatically reducing response time to incidents, improving resolution rates, minimising evacuations of USPS facilities, and disruption of mail processing activities. Additionally, and most importantly, these tools allow Postal Inspectors to give employees and the American public a prompt resolution to suspicious items resulting in renewed trust in the postal system.

FEAR OF WHITE POWDERS

The most common form of Anthrax is a white powder. This fact has resulted in numerous other harmless white powders found in a variety of settings being incorrectly identified as possible Anthrax. This paranoia, while greatly diminished from the early days of this crisis, continues to this day, often resulting in Postal Inspector response to harmless substances such as powdered coffee creamer, cornstarch, and other common and harmless materials. Generally these matters can be resolved quickly by responding Postal Inspectors by developing information including the location of the substance and any items which may be associated with the substance. Any questionable substance is promptly tested with specialised equipment including air monitors, radiation detection meters, portable x-ray units, infrared-based hazardous materials identification systems, as well as other sensitive

assessment equipment. Safety for the responding Postal Inspectors is of paramount importance and the main reason for use of Level C equipment for hazardous materials response. This level includes chemical resistant jumpsuits, protective over-boots, gloves, and positive-pressure respirators. Additionally, some Dangerous Mail Specialists, the designation given to Postal Inspectors trained in this area, are trained and equipped to Level B hazardous materials response which adds a self-contained breathing apparatus.

Because any actual biohazard attack is, in fact, a crime scene, all Dangerous Mail Specialists are not only first responders but also highly-trained criminal investigators. Dangerous Mail Specialists are trained and equipped to conduct forensic sampling and crime scene processing while in a hazardous materials environment.

These very significant efforts on the part of the USPS and USPIS to address this threat have been highly successful. Since the adoption and installation of the BDS, hundreds of billions of letters have been processed by the USPS and screened through this system. To date, there has not been a single alert or even false alarm in mail processing plant in the United States.

Similarly, suspicious mail item responses by Dangerous Mail Specialist since 2001 total more than 37,000. All of these incidents were handled successfully with only a few found to be actually hazardous and requiring an investigation.

DMI Suburban and tools

xrays of electric puppets and 2 bongs

MORE INNOVATIONS

The Anthrax mailings came during the immediate aftermath of the September 11 terrorist attacks. As the USPS moved to improve its state of readiness regarding threats being introduced to the 'mailstream', the threat of terrorism not directly involving the mail was also considered. In addition to the deployment of BDS and improvement to response to chemical, biological, radiological or explosive

City of Industry BDS Exercise 7-24-08 026

threats, the USPIS also developed and implemented improved threat mitigation, response, and recovery capabilities. Part of this additional effort included the deployment of a specially equipped fleet of mobile command centers to ensure we could manage operations anywhere in the United States regardless of the circumstances. The implementation of these additional strategic assets were instrumental in the USPIS successful response to the aftermath of Hurricane Katrina, which hit the Louisiana and Mississippi coast in the southern United States and destroyed much of the city of New Orleans.

The continuous use of the training and equipment developed as a result of the Anthrax attacks has also improved USPIS handling of mail screening at large public events, an activity the USPIS has engaged in for as long as it has been in existence. A mobile mail screening station for use at special events has been constructed and deployed. This unit is completely self-contained in a large tractor-trailer and can be use to screen mail to VIPs and others in large amounts and on a continuous basis. Yearly events handled by the USPIS using this equipment and specially trained Postal Inspectors include the Super Bowl, baseball World Series, Republican and Democratic National Conventions, and similar event. This equipment was most recently used to screen mail for officials, VIPs and athletes at the 2010 Vancouver Winter Olympic Games.

MOVING FORWARD

Postal Inspectors respond to reports of suspicious substances in the mail every day. While the vast majority of these response are false alarms resulting from accidental spills or leaks of chemicals that should never have been introduced into the mailstream, the response must be treated as a potential threat until it can be ruled otherwise. While Postal Inspectors know that even in those rare cases where a threat is confirmed it is unlikely to be an actual terrorist event. Most of the actual threats Postal Inspectors encounter are individual attacks that are personally motivated, often prompted by revenge or business disputes, however another terrorist attack on the postal system or using the mail cannot be dismissed.

For over 250 years Postal Inspectors have stood ready to protect the USPS, its employees and assets, and the mail from criminal attack, and the public from crimes committed using the postal system. While this proud legacy

comes from a long and successful law enforcement history, Postal Inspectors understand the reality of new threats against the USPS and are committed to continuing to lead in innovative and practical solutions to the new risks and threats we encounter.

EDITOR'S NOTES

Mr. Oscar Villanueva is the Deputy Chief Inspector, U.S. Postal Inspection Service (USPIS) and Assistant Chairman of Postal Security Group, Universal Postal Union. The USPIS is a close partner of the Home Team Academy – Ministry of Home Affairs. Since signing a Training Memorandum of Understanding (MOU) back in December 2008, both agencies have strived to further develop their working partnership.

Bioterrorism *and the* Role of Public Health

MS. PAMELA DIAZ

The World Health Organization refers to bioterrorism as "The use of biological agents in terrorism. This includes the malevolent use of bacteria, viruses, or toxins against people, animals, or plants"[1]. Microbiologic agents have characteristics that render them desirable for illicit use when compared to chemical or nuclear materials. They are easily concealed making them easily transportable and virtually undetectable during transport. And, under the right conditions, they can be propagated to large quantities, sometimes necessitating only basic microbiology skills.[2]

Recognising the potential risk that microbiologic agents could pose when used illicitly, "The Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases and of Bacteriological Methods of Warfare", known as the Geneva Protocol of 1925, detailed efforts to prohibit the use of biologic weapons.[3] This Protocol was the first multilateral agreement that extended the prohibition of chemical agents to biological agents. Subsequently, the Convention on the Prohibition of the Development, Production, and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction (commonly known as the Biological and Toxin Weapons Convention) banned the development, production, stockpiling, acquisition and retention of microbial or other biological agents or toxins, in types and in quantities that have no justification for prophylactic, protective or other peaceful purposes. It also banned weapons, equipment or the means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict.

Numerous microbiologic agents and toxins could be utilised to potentially cause harm. Perpetrators may choose one particular agent over another for a variety of reasons that could include their technical knowledge, availability of the agent and reagents, the ability to propagate and disseminate the agent, monetary resources or for other logistical

considerations. Depending on the purpose and method of the attack, certain characteristics of a biological agent may be more conducive to a particular attack's success than others. Some of these characteristics include stability of the agent, the ability to infect and cause disease using very small amounts, the lethality of the agent and the ability to disseminate the agent effectively.

THE ROLE OF PUBLIC HEALTH AND HEALTHCARE ENTITIES

The U.S. Department of Human Services, Centers for Disease Control and Prevention collaborates to create the expertise, information, and tools that people and communities need to protect their health – through health promotion, prevention of disease, injury and disability, and preparedness for new health threats. Other public health entities around the world, such as the Singapore Ministry of Health promote similar goals championing healthy nations through innovation and excellence to promote health and reduce illness. Public health entities such as these have roles in the response to events that threaten the health of the public regardless of the source of those events.

The role of public health entities in outbreaks of disease include detection of the outbreak through public health surveillance, confirmation of the etiology through the use and interpretation of laboratory tests, investigation of the outbreak and the institution of public health control measures such as treatment recommendations, isolation and quarantine measures when appropriate. Public health investigations of outbreaks of disease may be complex, particularly when the outbreak is caused by an emerging infection or the result of perpetrated attack. Depending on the event, the difference between a naturally occurring illness or outbreak and one that has been caused maliciously may solely lie in the fact that one is an act of nature and the other is a crime.

Biological events, whether naturally occurring or perpetrated, rarely have a definable scene (location) of the event like more overt events such as explosive or chemical incidents. Biological events are generally more insidious or covert, unless a perpetrated event is announced (e.g. envelope with a threat letter and an unknown powder) or a dispersal device is found. More likely, the first indication of the event will be sick individuals presenting for medical care. When an attack occurs, the time from exposure until the onset of illness in those affected may be several hours to days or weeks depending on the agent. This incubation period provides a

window of time for a perpetrator to release a biological agent and flee the scene before victims exhibit symptoms of illness.

During the early phases of the outbreak, when ill victims are initially presenting for medical care, a biologic attack may be difficult to differentiate from illnesses occurring from a naturally occurring outbreak. The first responders in this instance will be emergency department physicians and nurses, outpatient clinicians, laboratory experts and specialists in infectious diseases, infection control and public health.[4] Ill individuals will likely seek medical attention in multiple institutions depending on where they are when they become ill, some potentially very far from the exposure site.

Healthcare providers are the crux for reporting potential cases and/or events to public health entities. In the 2001 anthrax letter mailings in the United States, it was a clinician that was the first to alert public health of the first case of inhalation anthrax to be diagnosed in the U.S. since 1976.[5] And, in 2003, a global outbreak of Severe Acute Respiratory Syndrome (SARS) occurred resulting in more than 8,000 probable cases and 774 deaths in 25 countries as of July 2003 before it was contained.[6] Control of the outbreak required the efforts of public health and healthcare providers on an international level. Because of their characteristics and the role of public health and clinical sectors, attacks with biological agents require an additional dimension of emergency planning that involves including the public health infrastructure.[7]

OUTBREAK INVESTIGATIONS

Public health entities utilise sound epidemiologic, laboratory and forensic approaches to the investigation of outbreaks. They design and conduct epidemiologic investigations of outbreaks in order to answer questions regarding transmissibility (communicability), severity, extent and spread of the outbreak. Answers to these questions enable determining and promptly instituting public health measures and recommendations that are aimed at controlling the outbreak and preventing further illness. The success of these investigations hinges upon the close coordination and cooperation that exists between public health and medical sectors.

Naturally occurring outbreaks can have a certain amount of predictability in terms of consistency with previous occurrences and biologic plausibility. A number of epidemiologic clues to identify events that could potentially be the result of bioterrorism have been previously described[8]. Some of these clues include a single case of disease caused by an uncommon agent, large numbers of cases of

unexplained illnesses or deaths, unusual or atypical illness for a given population or group and unusual disease presentations[8]. Awareness of these clues can be helpful to public health officials when evaluating infectious disease outbreaks.

The clinical history including the history of symptom onset and progression as well as occupation, travel, recent activities and patient contacts provides valuable information that can lead to early hypothesis regarding the cause and of an outbreak. The first case of inhalation anthrax in the 2001 letter mailings of anthrax in the United States was an individual that did not have any of the known risk factors for inhalation anthrax. His occupation was in the news media and he had not come in contact with or participated in any activities that were risk factors for acquisition of the disease. Knowledge of this information quickly led public health officials to recognise that something was highly unusual about the case and to quickly launch an effort to identify any additional cases and investigate the situation[9].

INVESTIGATION OF BIOTERRORISM EVENTS

A BIOTERRORIST ATTACK IS by definition a crime and will necessitate and include a law enforcement investigation. Law enforcement investigations have additional requirements for assuring that evidence will be accepted in a court of law if the criminal is apprehended and tried. Adequate chain of custody ensures that evidence has a traceable history and is not contaminated along the way as it is processed from the patient or crime scene to the courtroom. In the situation of a bioterrorism attack, clinical specimens such as cultures or environmental swabs may become evidence. Standardised processes for handling and transport can preserve the integrity of the samples and also maintain appropriate chain of custody requirements.

In many countries, criminal justice systems may be constrained by inadequate legal frameworks governing the detection and repression of bio-weapons. Frequently, no law is violated until the biological agent is actually deployed. Developing the legal framework to address the criminal aspects and public health issues that will arise when a bioterrorist event occurs requires a cross-sectoral approach that involves the law enforcement community, public health experts, medical professionals, judicial experts and the public.

Public health investigation of naturally occurring outbreaks will rarely require the involvement of law enforcement entities. However, investigation of bioterrorism events will necessitate public

health and law enforcement to work together. Investigations will need to occur urgently with law enforcement threat assessments and public health interpretation being key elements.

Public health and law enforcement have specific yet similar goals when conducting investigations. Law enforcement officials want to protect the health and safety of the public as do public health officials. Additionally, law enforcement works to prevent attacks, apprehend and convict criminals. Public health entities work to prevent disease outbreaks, investigate outbreaks and stop further cases of disease from occurring through recommendations and implementing control measures.

PREVENTION

One key element to achieving these mutually beneficial prevention goals involves securing dangerous pathogens. Securing dangerous pathogens as a prevention measure generally equates with assuring safe and secure laboratories. Safe and secure laboratories help ensure the containment of hazardous infectious substances, protecting valuable research and commercial assets, minimizing the risk of accidental exposure or release and reducing the risk of crime and bioterrorism.

The U.S. Government has identified specific biological agents and toxins (i.e select agents), that could potentially cause substantial harm to human health and agriculture. Prior to the Select Agent Rule there were no facility requirements for licensing, registration, identification of facilities, uniform safety requirements for handling the agents and tracking and verification of the transfer of the agents.

INFORMATION SHARING POLICY AND PROCEDURES

When investigations are conducted independently, both public health and law enforcement entities may acquire information that is relevant to the other's investigation. Because of this potential, information sharing between public health and law enforcement has the potential to improve the timeliness of investigative findings and save lives. To be most effective, strategies for information sharing should be pre-determined.

Public health and law enforcement investigators have access to unique information that may be important to share during an investigation. Law enforcement typically handles intelligence regarding terror groups and organisations, processes threats, intelligence and collects victim information for case management. Public health conducts surveillance

to identify diseases clusters and outbreaks, epidemiologic investigations of outbreaks and utilises patient information such as symptoms, illness onset, and laboratory test results to determine the cause and answer critical questions about the outbreak. Typically, however, these agencies do not often work together.

Although the goals of public health and law enforcement may overlap, the methods utilised and constraints will often be different. Public health entities are often bound by privacy laws from sharing specific patient medical information. Law enforcement may be constrained from sharing sensitive investigative information. Establishing communication mechanisms *before* an event occurs and working out procedures in advance will provide time to identify and overcome many of these challenges.

Trust and credibility do not occur immediately but can be gained through the development of relationships and joint strategies for communication and information sharing. An effective way to work through these differences is by joint planning and routine interactions. Developing triggers for communication and notification is a critical first step to building that trust and credibility. Protocols and procedures should be jointly developed to identify the circumstances when one entity would communicate with the other about a particular event or circumstance. Both agencies will need to identify mutually agreed upon thresholds when information would be shared between each agency.

Examples of triggers that could be considered for public health notification of law enforcement include test samples submitted to labs that are positive for agreed upon agents of concern, unusually large numbers of patients with similar symptoms or disease presenting to health care providers or unusually large numbers of unexplained symptoms, diseases, or death. Likewise, law enforcement triggers for alerting public health might include intelligence or investigative information indicating individuals or groups unlawfully possessing a biological agent, seizure of a biological dissemination device and/or assessment or threats that indicate a credible threat exists.

Once inter-agency notifications are made, public health and law enforcement next steps can move to conducting a joint threat assessment to determine if they believe a credible threat exists and determining the next steps. Joint threat assessments benefit by opportunities to further share agency specific information such as criminal history, intelligence, criminal case information from law enforcement and ongoing surveillance data, information on

disease, biological agents and disease expertise from public health officials.

JOINT INVESTIGATIONS

Because of the nature of a perpetrated biological event and the need for multiple sources of information and expertise, conducting a joint investigation should be considered when indicators are such that further investigation is warranted. When agreeing to conduct joint investigations and the sharing of information between agencies, both must take into account national and local laws including those that address privacy rules and criminal prosecutions. Because many countries have laws that protect patient confidentiality (sensitive medical health information), when developing protocols, legal counsel should play a role in ensuring that any protocols developed fit within the legal system where they will be implemented and may need to be consulted during an investigation for specific situations not previously described or agreed upon.

Joint investigations can provide many benefits to both public health and law enforcement entities. Law enforcement can benefit by having access to infectious disease subject matter experts and relevant health information. Public health can benefit by having access to potential specific law-enforcement case information (i.e. location of release, dispersal device used, targeted victims) and providing information that assists in the apprehension of suspects, therefore preventing future attacks that might result in further exposures to the agent.

JOINT INTERVIEWS

Generally, when interviews of sick individuals are needed as part of an investigation, certain information such as whether the illness or event is consistent with a particular agent, when an exposure might have occurred, where an exposure could have occurred, and how an exposure might have occurred is generally best collected and assessed by a public health expert. Whether the ill person may be the victim of the crime or the perpetrator of the crime is generally an assessment that law enforcement performs. Hearing the same information at the same time from the ill person and leveraging the skill sets from both public health and law enforcement simultaneously to acquire and synthesise the information can lead to findings and conclusions that neither one would discern independently. Another consideration for conducting a joint investigation is that, depending on the given situation, there may be a narrow window of time that an interview can be conducted before the individual becomes too ill to respond and/or dies.

Much of the information that is needed by public health and law enforcement is the same, but both entities have different priority information requirements that will help them to achieve their objectives. Each agency will bring a unique approach and perspective to the interview that may enable them to observe and garner clues differently resulting in mutual benefits. In addition, obtaining the information jointly can minimise the potential for obtaining conflicting information while maximising the opportunity to leverage the public health and law enforcement knowledge, skills and interpretation.

When conducting joint interview, predetermination of who leads the interview, how the patient will be approached and other key logistical elements should be worked out ahead of time.

> Regardless of whether information is obtained jointly or not, it is critical to have protocols and procedures in place to enable the sharing of information.

TRAINING AND EXERCISES

ONCE JOINT STRATEGIES, protocols and procedures are developed, joint training and exercises will provide the opportunity for public health and law enforcement to test protocols and refine them prior to an event. Joint exercises can help identify issues, gaps and inform further planning efforts.

SUMMARY

IN SUMMARY, BOTH law enforcement and public heath entities share many mutual goals and objectives. Both entities have roles that are critical to the successful outcome and management of a bioterrorist attack. Developing pre-planned protocols and procedures for sharing of information have the potential to improve the outcome of the investigation. Providing joint opportunities for training and conducting exercises can lead to further enhancements to these plans and lead to improvements in response during a real event.

REFERENCES

1. World Health Organization (Internet). Geneva, Switzerland. Available from http://www.who.int/topics/bioterrorism/en/
2. Moran GJ, Talan DA, Abrahamian FM. Biological Terrorism. Infect Dis Clin N Am 2008; 22: 145-187
3. Geissler E. Biological and toxin weapons: research, development and use from the Middle Ages to 1945. In: sipre Chemical and Biolgoical Warfare Studies. No.18. Oxford University Press: New York, 1986.
4. Henderson DA. The looming threat of bioterrorism. Science 1999; 283:1279-1282
5. Bush LM, Abrams BH, Beall A, Johnson CC. Index case of fatal inhalational anthrax due to bioterrorism in the United States. N Engl J Med 2001; 345(22):1607-1610
6. Rothman RE, Hsieh YH, Yang S. Communicable respiratory threats in the

ED: tuberculosis, influenza, SARS and other aerosolized infections. Emerg Med Clin of NA 2006;24:989-1017

7. Khan AS, Levitt AM, Sage MJ, with the CDC Strategic Planning Workgroup. Biological and chemical terrorism: strategic plan for preparedness and response. MMWR 2000; 49 (RR-4): 1-14
8. Treadwell TA, Koo D, Kuker K, Khan AS. Epidemiologic clues to bioterrorism. Pub Health Rep 2003; 118:92-98
9. Jernigan DB, Raghunathan PL, Bell BP, et al. Investigation of bioterrorism-related anthrax, United States, 2001: epidemiologic findings. Emerg Infect Dis 2002; 8(10):1019-1028

EDITOR'S NOTES

Dr. Pamela Diaz is the Director of Biosurveillance Coordination in the Public Health Surveillance Program Office at the Centers for Disease Control and Prevention (CDC) in the U.S. She represents CDC at international Bioterrorism training workshops sponsored by Interpol and the U.S. Department of State, providing expertise and training in joint public health and law enforcement investigation.

Dr. Pamela Diaz presented an excellent and highly thought-provoking session during the U.S and Singapore Bioterrorism Workshop in Singapore back in 2007.

She has been a front-line public health responder and was deployed to New York City for the 2006 inhalation anthrax case in an African drum maker and to Mexico City for the H1N1 investigations. She has provided consultation to the U.S. Departments of Health and Human Services and Homeland Security on matters related to infectious diseases and preparedness.

Dr. Diaz received her medical degree from the University of Toledo, College of Medicine and completed a fellowship in Pediatric Infectious Diseases at Stanford University. Prior positions include Assistant Commissioner of Infectious Disease and Public Health Preparedness for the Chicago Department of Public Health, and Assistant Professor in the Division of Pediatric Infectious Diseases at the University of Chicago. Her major interests include public health, emerging infections, methods of disease surveillance, public health preparedness and response.

Suspect Detection System:

A Detective and Preventive Forensic Tool

DR. VAYA, MR. NILESH, DR. DEVVARTA
(Gujarat Forensic Sciences University)

In the last two decades, rapid advancement in the field of information technology and overall growth in the economy has led to significant changes in the quality of life. At the same time, changes in the nature of crime including heinous terrorist attacks reflect the change in the attitude and mindset of the perpetrators. Growing terrorist attacks have become both a national and international concern as the cause is of either an 'ideological' or 'organisational' nature. That is to say, perpetrators carrying out these attacks may not have any criminal history which can render them as suspects to the law-enforcement agencies on the basis of their history. They may enter a country with just an intention to carry out an attack (without carrying any arms or ammunitions on them) and execute the group's intention with their local network once they are inside the country. Secondly, the attacks may be intended mainly to seek the attention of masses, thus the target may not be specific. Therefore, it is essential that security agencies are well-equipped with advanced technologies to nab these people with ill-intentions, and it is the need of the hour to master this art.

Forensic psychologists play a key role in aiding crime investigations. Past experience has shown that in order to prevent or tackle an organised crime, ways and means adopted by the perpetrator as well as the strategies designed for the execution of criminal activity must be understood. The work experience of [forensic psychology division at the Directorate of Forensic Sciences (DFS), Gandhinagar, India] handling nearly 5000 suspects referred for various psychological techniques of investigations in the last three decades has helped in understanding how the mind of a perpetrator works,

how it can be assessed and last but not least, how the perpetrator also needs psychological help for handling his own conflicts, and managing his thoughts and emotions in a way the prevention can be done.

Apart from working with criminals, a forensic psychologist carrying out his/her role in crime prevention efforts also requires technological help for the purposes of:-

Identification:

This warrants a technology capable of identifying the motivation, intentions, and behaviour of a person by focusing on the thought structure, process and pattern (formation) and preceding ideas before they crystallise to clear thinking. This process is like a blueprint of intentions. In the initial stages, if "thought blueprint" can be tracked and identified by the technology, a halt can be put to the thought process before it is coloured with emotions and ready for ignition by the belief system of the person. If adequate preventive forensic care is given by way of counselling during this state, it can save a person from becoming a probable perpetrator of crime.

Prediction:

In case of failure to identify them at the initial stage, crystal clear thoughts coloured with emotions may become "passion" waiting to be ignited by the individual beliefs for a congenial opportunity for outbursts. Where approvers are found with similar thoughts and beliefs in the social milieu, an intention with ignited emotions drives like-minded people for action. By then, the intentions are crystal clear and ill-driven by the belief, culminating in negative emotions. Approval in the individual's social milieu motivates the planning of the outburst and decides the target. The transformed crystal clear ill intention entailed with negative emotions supported by the social milieu provides a sense of belonging and helps in strategically designing the plan of action.

Prevention:

If technology helps in detecting at this stage, the impending outburst can be prevented, aborted or thwarted by not allowing the ill-intent to become ripe for an action. This can help in preventing the person from becoming a perpetrator. It can also help in unearthing the future course of action (i.e. identification of planned strategies and/or involved persons).

Detection:

In case of failure to identify these thoughts at the aforementioned stages, and there is a catastrophic attack, investigation starts and a

useful technology should be capable of detecting only the perpetrator from large number of suspected persons in a short span of time in a reliable and accurate manner. The technology should have proven scientific base, and be user-friendly without any discomfort for the examinee undergoing the test. It should be capable of giving direction to the investigation by correctly identifying the perpetrator. This calls for a technology capable of screening the intentions to identify the ill intentions in the mind.

Predicting future course of action:

IF IN SPITE of all preventive measures, when an attack takes place, it is essential to detect individuals harbouring hostile intent in real time to change the probability in favour of law enforcement agencies. From the suspects harbouring hostile intentions, detailed investigation should help in unearthing strategies and plans of likely targets which can be verified and helps in achieving crime-related intelligence.

Different types of polygraph instruments, Electroencephalograph (EEG)-Event Related Potentials (ERP) instruments adjunct to forensic psychological assessments are used for eliciting physical correlates for comprehensive forensic evaluation of the suspects. The scientific base involves either psychophysiology, electrophysiology, or neuropsychological methods for eliciting physical correlates for forensic purposes.

Recently, a high tech, handy, portable, user-friendly screening device from Israel was technically evaluated at (DFS), Gandhinagar. It is an Autonomic Nervous System's (ANS) reactions-based suspect detection instrument. It is established that various ANS parameters such as the Galvanic Skin Responses (GSR), Heart Rate, Blood Volume Pressure (BVP), respiration rate and so forth react to the conscious efforts of deception (Lykken, 1959; Raskin, 1989; Bartol & Bartol, 2004). Among these, the GSR and BVP measures are used by Suspect Detection System (SDS). The SDS is based on the assumption that an individual can be stimulated to generate psychophysical reactions to crime-related triggers (e.g., words or sentences). Furthermore, those with a desire to hide a criminal intent will have different Stimulated Psycho Physical Reactions (SPPR) from the SPPR of people not having such intent. The SDS can be used for the purposes of identifying a perpetrator of a criminal act from the group of suspects. For this, it uses the Guilty Knowledge Test (GKT) paradigm (Lykken, 1959, 1960) which is based on the assumption that if an individual has committed a crime,

then his SPPR of the triggers related to the Relevant Stimulating Objects (RSOs) will be different from the SPPR of the RSOs of non-involved or innocent persons.

DETAILS OF THE SYSTEM

SDS is a compact, user friendly tool. It includes a briefcase consisting of a laptop, headphones, and skin-conductance sensor. This feature gives mobility to the user so that it can be used in various settings. It includes the software which analyses a galvanic skin response of the individual and also provides results on the basis of analysis. It does not require any other external device or tool for analysis.

The examinee is requested to sit comfortably, place his or her palm in a sensors cradle, put on headphones and answer several sets of questions. Questions are presented both in text and audio mode by the system, while the sensors measure psychophysiological responses.

Two types of questionnaires are prepared, one for screening and the other for investigation. These questions are prepared and fed to the instrument in advance. There are six sets of questionnaire in each screening test and each set comprises six questions. Initially, only four sets comprising 24 questions are used to stimulate examinee's unconscious reactions. Questions are different in terms of the individual's involvement. The examinee is instructed to answer the questions accordingly depending upon the nature of the questionnaire. Even if the examinee does not wish to respond verbally, the system picks up the signals of GSR from the finger. The test process takes about five to seven minutes and after the completion of the test, the decision will be made to classify the individual as suspect or non-suspect. In cases where the examinee is found to be a suspect, further information for directions of investigation is provided by the system and the system will automatically present an additional two sets of questions in order to reduce false positive cases. In the investigation mode, there are four sets of questions. The system records both audio and video inputs during the test. The procedure of using this questionnaire is akin to that of the screening mode. The basic input which is required to analyse the guilty knowledge is the individual's skin conductance. Through Galvanic Skin resistance sensor, the individual's responses are picked up by the system.

Responses collected by the system are analysed by the software, on different parameters. These parameters pick up signals of tension, response delay, latency and amplitude of the response, and the individual's biofeedback mechanism. These are unique sophisticated parameters of the system which make it more

sensitive for forensic purposes. The responses collected are intended to compare between baseline reactions and reactions to incidence-related questions. While analysing, the related questionnaires are compared with non-related questions. All these parameters are analysed using algorithms; Fuzzy Logic, Neural Networks and Pick of Tension, which are effective in measuring biofeedback and psychophysiology. This algorithm combines the results of all these parameters and offers the following results:

- The strongest reaction and the second strongest reaction generated by stimulus
- The strength and validity of each reaction
- Tampering attempt by the subject

The result of the system is given on the basis of the analysis of 14 different parameters. Additionally, software also validates the responses and informs on the validity of that specific response to the specific question. The validity helps in understanding the physiological as well as external factors affecting the results.

The tool also helps in understanding the results when a person is under influence of any substance, or trying to tamper the result. As it is based on neural network mechanism and biofeedback, the instrument measures baseline on the basis of the individual's responses given to the questions. Any substance or tampering is not taken into consideration while analysing the final results, which is in a way measure of validity while measuring output result that is suspect or non-suspect.

SDS AS A SCREENING TOOL

When an investigator is not clear about the role of the examinee in the crime, the screening which takes less time and helps in minimising the investigation can be done instead. Investigation is more specific to the crime or incidence.

> To identify the role of a suspect, investigation is done. It helps in understanding the information about the crime which is known not to others but the perpetrator only.

Technical evaluation of the SDS was done at the DFS, Gandhinagar, India, focusing upon the feasibility of its use for security purposes. Simulated experiments were conducted using the SDS to see its efficacy in detecting suspects and non-suspects (Wagh & Vaya, 2009). Twenty college students aged between 20 to 25 years, who volunteered for the study, were included and randomly distributed in two groups – experimental and control groups with both having an equal number of subjects. The

experimenter who had to assess the subjects on the SDS and to decide on the basis of the SDS results about a subject's suspect or non-suspect status was blind to the group status of the subjects.

The experimental group subjects were briefed about the task they were supposed to perform. The task comprised of first watching a video clip about the procedure to prepare an explosive. After watching the video they had to go out of the lab premises, prepare a fake explosive (with dummy materials) and place it in the premises without others' knowledge. The control group was not exposed to any video and were not instructed for the task that the experimental group had to do.

After the completion of the task by the experimental group, subjects of both the groups were assessed on the SDS. The results indicated that the instrument was successful in detection with almost 95% accuracy.

Furthermore, when five to six suspects were subjected for screening in blast cases, the system suggested probable belongingness of the identified suspects to a specific organisation, probable source of funding, future course of action, probable time and places of future terrorist attacks. The results of these suspects suggested that it is a useful and time-saving method to gathering intelligence. Timely screening can help in preventing the catastrophes, aborting the course of action by thwarting the ill intentions. The preventive forensic aspect of detection helps in saving an individual from becoming a criminal.

CONCLUSION

THE SDS IS an effective screening tool for the identification/detection of a person with ill-intentions which can be further investigated on the basis on the results and the gathered information can be used for the purpose of prevention of further crime as well as the perpetrators of crime.

SUGGESTIONS

FUTURE STUDIES ARE required to validate its efficacy in countering the measures to suppress the ANS reactions to deceptions, often used by people undergoing these types of examinations.

REFERENCES

1. Bartol, C.R., Bartol, A.M. (2004). Introduction to Forensic Psychology. California: Sage publications.
2. Lykken, D.T. (1959)The GSR in the detection of guilt. Journal of Applied Psychology, 43, 385-388
3. Lykken, D.T. (1960) The validity of the guilty knowledge technique: The effects of faking. Journal of Applied Psychology, 44, 258-262.
4. Raskin, D.C. (1989). Polygraph techniques for the detection of deception. In: D.C. Raskin (Ed.). Psychological methods in criminal investigation and evidence. New

York: Springer-Verlag.
5. Wagh N. B., Vaya S. L. (2009) Suspect Detection System: Fast Track Method for Screening the Suspects. Proceeding of XX All India Forensic Science Conference, Jaipur, Rajasthan, India. 771-778.

EDITOR'S NOTES

Dr. Vaya Shivarathna L., Wagh Nilesh B. and Devvarta Kumar are part of the team at the Institute of Behavioral Science (IBS) of the Gujarat Forensic Sciences University (GFSU). IBS's mission in India is to impart education and to undertake research in clinical and forensic areas, while at the same time, provide the highest calibre in diagnostics, psycho-legal consultation to referral sources (clinicians, attorneys, the Courts, social service and criminal justice agencies etc.) and treatment and rehabilitation to clients.

Dr. Vaya is an Additional Director at the Directorate of Forensic Science (DFS) and Director IBS at GFSU. Her areas of research include work on the standardisation of psychological tools for the Indian context. Her other major research contributions in India include her work on Normative Data for Brain Electrical Oscillation Signature (BEOS) Profiling, the National Resource Centre (NRC) for Forensic Psychology and on the Competency to Stand Trial (CST) system. She has been invited to deliver lectures on forensic and investigative psychology by international, national and state investigating agencies. She is the first accredited officer for Polygraph Examination, Narco-nalysis and BEOS Profiling at the Indian National Accreditation Board for Testing and Calibration Laboratories (NABL), She has a Diploma in Medical and Social Psychology, Bachelors and Masters Degree in Clinical Psychology and Doctor of Philosophy (PhD) in Psychology.

Mr. Nilesh is a Junior Assistant Professor in Clinical Psychology at IBS. Major research areas he is working on presently also include the BEOS and CST system as well as the Suspect Detection System (SDS). He has delivered lectures on forensic psychology for Indian judiciary and police officers. He is a recognised operator of the SDS as well as the Cogito Operator-Advanced (C.O.A) System. He has received his Bachelors and Masters Degree in Clinical Psychology and a Masters of Philosophy (M.Phil) in Medical and Social Psychology.

Mr Kumar is also an Associate Professor of Clinical Psychology at IBS. His primary research interests are memory and other cognitive impairments in schizophrenia, non-pharmacological intervention in psychosis, norm development of psychological tests and lie-detection. He is the author of about twenty articles in journals and books. His education includes a Ph.D. in Clinical Psychology and a M.Phil in Medical and Social Psychology.

"*Innovating* and *Fostering Creativity* in **Homefront Security**"

MR. PETER HO HAK EAN
Former Head Civil Service,
Permanent Secretary,
National Security and Intelligence Coordination
and Permanent Secretary,
Ministry of Foreign Affairs
10th March 2010

Interviewer: *PS, welcome to the Home Team Academy. We are very pleased to have you share with us your perspectives on the changing landscape of Homefront Security in Singapore and more importantly, how we can leverage on innovations and foster a culture of creativity.*

Among your several key office appointments, you have been the Permanent Secretary at MINDEF and you are at present concurrently the Permanent Secretary for Foreign Affairs and Permanent Secretary, National Security and Intelligence Coordination. Now, from your experience at the helm of these key ministries, what do you see as the most significant changes in Homefront Security?

PS: I would go back in history to the time when the Ministry of Defence, and what we know as the Ministry of

Home Affairs, was a single ministry – the Ministry of Interior and Defence. The government took a decision to split these into two separate ministries, so each could focus on the specific areas. The Ministry of Defence focused, obviously, on defence. This was to facilitate the build-up of our defence capability and this was during the period when National Service was introduced. And of course, the new Ministry of Home Affairs, focused on law and order. I think that proceeded for a couple of decades. A big change, I think, took place when the Ministry of Home Affairs created this concept of the Home Team. And I thought that was a very major mindset breakthrough.

Interviewer: *That was essentially the milestone, wasn't it?*

PS: Yes. I thought that was a milestone, not because overnight it changed things but what it changed was to alter the way people within the different groups looked at their work – they no longer saw their job as policing work or civil defence or prisons or CNB (Central Narcotics Bureau). They saw themselves as working towards a larger goal, as part of a much larger team. And of course, it takes many years for this kind of mindset to change, but I think that was the beginning. I think what happened after 2001 – and I'm not just talking about the September 11 attacks, I'm also talking about the December 2001 arrest of the JI (Jemaah Islamiyah) people – was that it became very clear that for us to deal with this new kind of threat, we could no longer operate within our silos, or within the mission defined for each individual ministry.

The security landscape has changed completely. We would have to get the Ministry of Defence, the Ministry of Home Affairs and indeed, other ministries like the Ministry of Transport, Civil Aviation, the Maritime and Port Authority, Land Transport Authority, all coming together to tackle a new and very complex problem. I think the fact that the Home Affairs had already started this process of thinking of how they had to work together with others made it much easier for them to transition in the end from thinking about the Home Team to thinking about the 'whole-of-government' theme. So I think that was very critical, the concept of the Home Team made it easier. That's not to understate the difficulties of getting agencies to work together. That involves having to deal with the complexities of human nature.

Interviewer: *I can imagine that it would have been a long arduous road to achieve this…*

PS: There will be turf battles initially. Lots of fights and indeed that happened in the beginning. But

I think after a while you could really see that the agencies came together and saw that there was a mission that no single agency could meet on its own. They came to realise that it was easier to work together – that this was a national mission and therefore they had to commit resources, and put their heart and soul into it, even though this might not fit tidily into their own separate mission. So I think that was a good development.

I would say that there have been other governments which have taken a slightly different approach. The US Homeland Security combined something like 25 agencies from different departments to create the Department of Homeland Security, in the hope that they would be able to meet this new mission. Of course the problem with this is first, resource. Second, the departments have other priorities as well. But if you have a department that is dedicated to Homeland Security, what about their other responsibilities? So something has to give. So our approach has been slightly different – let's try to operate in a matrix, whole-of-government fashion and try to create a mindset in which people give as much commitment to their responsibilities in this network of cooperation as they would to their own statutory board or their own ministry. We've moved quite a way beyond that and I know – I was in the thick of it in the early part – how very difficult it can be to create this mindset. There were, very clearly, big turf battles, though everybody would deny that those things happened in Singapore.

Interviewer: *That was the reality wasn't it?….*

PS: But that was the reality of how it was. And everything was couched in very noble language, that *"we are not doing this because there are other important things to do and we've got our priorities."* But of course, in the end, it boils down to the turf battle, protecting turf. They might say, *"not invented here – if it is not my idea, I am not going to support…"* So that was the reality.

Interviewer: *It was obviously a big internal challenge, and I can see from what you've told me, how this is an incredibly fine balancing act. In view of these challenges both internal and (the internal aspect is quite big), and of course external, faced by all our Homefront Security agencies these past few decades, what do you think are some of the noteworthy innovations or developments that happened during this period or as they evolved, that particularly impressed you?*

PS: I give you one specific example, both to illustrate your point, and to show how in the end we were able to change mindsets. The example

is Jurong Island. Very early in the day, we realised that Jurong Island was both vulnerable to terrorist attacks and it was an island very important to Singapore's economy. Therefore it had to be protected. But it was designed for safety, not for security. So we said: *"Well, this is an immediate problem, we better do something about it."* And I remember, we did some very quick studies and in fact, the study showed that if there was an attack in the right places, the consequences could be quite catastrophic. So we met the people in charge of Jurong Island – JTC, the Ministry of Defence, the Ministry of Home Affairs, Police, SAF and so on. And the conclusion was we needed to do something about it and the immediate consequence was to put out SAF and police patrols. That was the quick and dirty solution. Later on, we said: *"Well, this is not a sustainable approach..* You can't sustain that kind of thing and those kinds of numbers in terms of deployment and with the number of companies involved. So we said we needed to spend money to build some kind of security infrastructure, including a proper facility to check lorries, people coming through….

Interviewer: *Something sustainable and manageable…?*

PS: Something sustainable. Some fencing, watch towers, cameras and so forth. So you have to spend money. I remember the bill came up to something like 40 to 50 million dollars. I told JTC and MTI: *"You should spend the money, because it is in your interest to do it. This is to protect your assets, your infrastructure."* And I said to them: *"Let's look at it from a different point of view. This will be your competitive advantage because in the end, people put money, in this new world of protection against transnational terrorism, where they believe that their investments, infrastructure and assets can be protected. So this will become your selling point."*

Interviewer: *And of course investors are very much interested in knowing that their assets are secure.*

PS: Yes, they want to know that their assets are secure. So I told them: Go and spend the money. I can imagine some initial natural reservations as some money might have to be taken out from other projects. But in the end, they had a reasonably good protective capability around the island, not perfect, but a reasonably good one. And quite soon, they discovered that this really was their competitive advantage, and they started to use it as their selling point. And I illustrate this point, to explain how difficult it is to change people's mindset and I am simplifying what was a very hard process to achieve

this. I mention this also because if you talk about innovations, it is not always the obvious, such as putting up fences, checkpoints and those kinds of things. Those are not very innovative. The innovation is to come up with the concept and framework to justify these things. And so the innovation here, was the idea that *"this is your competitive advantage."*

Interviewer: *Essentially, you had to convince people that it is in their interest….?*

PS: I had to convince people that it is in their interest and once they half believe it, then things will start moving along. But you must come up with a concept first. Technology is the least of the problems.

We were of course, very worried about the security of our seaward approaches to Singapore. And while it is relatively easy to monitor the movement of the large ships, it is much more difficult to monitor the movements of harbour craft. There are so many more of them, moving all over the place, moving relatively quickly. So there were two innovations. One was to have defined routes for ships and boats to take. If you are not in those routes, then you should be investigated. This was particularly important, in terms of the movement of ships near sensitive installations[1], whether it's Jurong Island, Bukom or anywhere that is a sensitive installation at sea. The solution to the problem of harbour craft is a 'no brainer': simply put some kind of transponder on the harbour craft. And again, somebody said, "Well, how can we do this cheaply?" The reply to this was, "Let's use GSM[2] technology." That was exactly what they did because these small craft are all within range of our GSM network. So it's not a problem.

Interviewer: *So essentially we tapped into an already available solution?*

PS: The solution was available there. You just need to do a bit of work on it and you've got something. The system costs roughly about a few hundred dollars. The innovation here was going to be how do we persuade the harbour craft to do it?

Interviewer: *The same question crops up again, how do we ensure cultural buy-in?*

PS: Yes. How do you get them to buy-in? We felt it would be not sustainable for the government to pay for these transponder systems. Not because each unit is expensive, but there will be new craft coming in, there will be requirements to replace old transponders. So again, the innovation is very simple. You simply make it a condition of license. For the first lot, the government will pay for

it. After that it becomes a condition of license. So if you want to renew your license to operate as a harbour craft, you must also agree to put and install these parts, namely the transponder system and you must be prepared to pay for it. Hence the problem was solved.

Interviewer: *I suppose the intention is to make one realise that the whole package for getting the license involves incorporating these security measures?*

PS: So the whole package is this: If someone wants the privilege of operating a harbour craft, getting the transponder is part of the entire package. So, when we think of innovation, we should not just be thinking about innovation in terms of technical innovation, or process innovation, we should look at policy innovations. Because you need policy innovations in order to support some of these systems and ideas which you want to implement. So what's the policy innovation for harbour craft – it's the licensing innovation. What's the policy innovation for Jurong Island – it's the policy innovation of saying, *"That's your competitive advantage."* So let's not just think about policy innovation at just the small level, because the policy innovation is as critical as the technological innovation or the process innovation.

Interviewer: *If not more so at times…?*

PS: If not more at times.

Interviewer: *And it brings us very nicely to the next point, because, many of these policy innovations, cannot operate in isolation, you can't just look at our own internal environment but also at what's happening outside. Quite naturally, in this globalised world that we now live in, it's very important that we adopt an international outlook to validate and improve these local capabilities that we just talked about. Now, we are not alone and we have a lot of partners, foreign counterparts. I am just wondering how we can actually learn from them as well?*

PS: I guess, be very open-minded. You must go out to actively look for people who have new ideas. You must meet people of all kinds and sometimes they've got harebrained ideas, sometimes they've got very good ideas.

> You must know how to filter out the wheat from the chaff, but at the same time look at their ideas. Don't reject them unnecessarily out of hand. Be prepared to meet people.

But if you try to take in everything, you have no time at all to do anything

else. You must know how to filter out the wheat from the chaff, but at the same time look at their ideas. Don't reject them unnecessarily out of hand. Be prepared to meet people. My operating principle is not to just focus on what the international community has to offer. They've got good ideas, but also to look at what we are able to do locally. We cannot say that we don't have our own ideas. In fact, one of the dangers I think, is to believe that all the best practices are to be found overseas. I think we have reached a stage where many of the best things which are being done, are being done here.

Interviewer: *In Singapore itself…?*

PS: Yes, locally. We don't need to look beyond our shores to find best practices or to find good ideas. Taking the example of the Home Team, I've visited the SCDF (Singapore Civil Defence Force) many times and it is a source of great admiration to me, to see how the SCDF has relied on its own people and its own sense to innovate and create some truly innovative products – such as the Red Rhino and many other equipment. These are not ideas which they've gone overseas to source for. They believe that they are as good as anybody else. They believe their ideas are as good as anybody else's. They believe they can translate these ideas into workable products, and they do it. So, more of our people should have that kind of a mindset. So I think maybe we should look both inside, and outside, for ideas. We must spend time looking and thinking. Don't close off the search but we must be prepared after a while, to say, "Okay, let's try it." Even if it isn't 100%, it doesn't matter. Don't say it's a failure. Say, "Okay, this is something which works, but can we improve on it?" So when moving in such a direction, always have a problem solving mindset that does not aim for 100% immediately. Let's try to get it from 70% to 80% to 90%, finally to 100%.

> When we think of innovation, we should not just be thinking about innovation in terms of technical innovation, or process innovation. We should look at policy innovations. Because you need policy innovations in order to support some of these systems and ideas which you want to implement.

Interviewer: *I suppose to allow it to work with the ground reality and see how it goes….*

PS: Let it work, see how it works and don't aim for perfection at the start.

Interviewer: *Yes, that will come later; you improve as you go along.*

It's interesting that you should mention that, because you are very correct to say that many of these solutions sometimes can be right under our noses. Sometimes what our officers need is just that opportunity. Moving on from that point and the whole idea of fostering innovation and a culture of creativity…. the notion of having to innovate is not a very new concept. It's been repeated many times in different contexts and often it can run the risk of becoming rhetoric and routine. Now I'm just wondering, how can we actually encourage this culture of innovation and creativity among our Home Team officers, without them thinking it's being imposed on them?

PS: Well you cannot really impose innovation because people are not going to be innovative because you tell them: "Look, your KPI is to be innovative," or "Look, I order you to be innovative." It has a lot to do with a framework you establish within the organisation. It has a lot to do with what the leadership itself does to facilitate new ideas to surface, to help translate, and to encourage these new ideas to be translated into something workable. I go back to the example of SCDF. I'm quite sure it is not because James Tan[3] at that time said, "Go out and innovate." So, will they innovate? The answer is probably no.

You need a lot more than that. You need a system in place, which allows people to surface their ideas and then, you need to create some kind of critical mass around these ideas so that these can be translated into some piece of equipment or some new process. You are doing this all the time through WITS[4] and the Staff Suggestion Scheme – the kind you see in organisations like the SCDF. Then I think it's got a lot to do with the quality of leadership and what the leadership itself encourages. There is no single template and I'm sure it starts off with *"I've got a problem – now what's the solution?"*

It's a simple question – *"what's the problem, what's the solution?"* Now I can ask someone to tell me what they think the solution should be. Getting the right type of people? The right type of encouragement? They might come back to me and say, *"well, okay, I think I dreamt of this idea of a 'Red Rhino'[5], that's it."* Now what does the leader do? If he says, *"yes, thank you very much"* and then files it away, that would be the death of innovation.

Interviewer: *I can see how it always has to start with the problem at hand and asking those very simple questions like, "this is the problem, what are the immediate solutions we have around us"…… but just to tap on this idea of 'problems', because a lot of these problems are not always internal, some of them are happening as a result of our rapid globalisation in all arenas – both the economic*

and political. In today's climate we're getting a lot of new challenges, stemming from let's say, new media, a burgeoning foreign population and of course an outward and very expressive younger generation. I'm just wondering, all these challenges that are coming, both internal and external, what do they pose for our Homefront Security landscape?

PS: Well, clearly it will require new types of responses. It will require new skill sets and new capabilities among the people who work in the Home Team. But all the values which you consider important will still be there. Furthermore, you're definitely dealing with the population that is more demanding, has much higher expectations of the Home Team and of the individual services within the Home Team. They will be less tolerant of failure; they will be less tolerant of poor service standards. I think that means your ability to deal with the community – face to face, through the new media – will have to be enhanced. I think you cannot have police officers in future who are unable to both communicate through the new media or deal with problems face to face. You must have both skills; you can't have one without the other. I think there is another important skill set that is becoming more and more important. You mentioned that we live in a globalised world and increasingly our problems are therefore globalised problems. Whether it is transnational terrorism or our concerns about security in the aviation arena, there are concerns about the movement of strategically sensitive material, criminals crossing borders around the world, money laundering, and so on. These issues require a lot of cooperation with authorities, not just in neighbouring countries but internationally. It requires cooperation with global organisations such as, INTERPOL. So it means that more and more, our people in the Home Team will have to think not just about the local issues. They have to think about global issues. They must feel comfortable, not just operating in the local domestic environment but equally comfortable operating in a global environment. The skill sets required for this are different. In the local environment, you are in full control. You got the regulations and legal statutes to back you up; you can control things more or less. You go overseas, it's quite different – you are one of many, you need to have the social skills, the EQ and the confidence to deal with your counterparts with confidence and with authority and I think these are going to be skill sets that we will increasingly expect of our people.

Interviewer: *Yes, I can see how we can of course dictate a lot of things if they are internal to us, but many*

of these issues and problems which require cooperation outside our borders require an entirely different set of skills that are not just technical but more people based.

PS: Our Home Team officers will have to cooperate and work with them. That's already happening among the intelligence agencies. For instance, ISD[6] and the police in their dealing with their counterparts. In fact, we can see our police officers deployed in places like Timor Leste and in the last couple of decades they've been all over the world.

Interviewer: *I think we have taken a big step in that direction and the road ahead looks very promising. But of course there are going to be a lot of challenges to overcome. In light of all these current trends and developments, can you tell us what you think is the single most current and innovative solution that is basically helping to address these issues?*

PS: I personally believe that our competitive advantage is going to come from our ability to work at a 'whole-of-government' level – in a *networked* fashion. In other words, we don't just take the point of view of one individual agency or individual ministry or individual service. But we also try to contextualise what we do to the larger national interest. This is not just an academic or intellectual exercise. It is something we must truly believe in and must be prepared to act on and this is what we are moving towards.

We have to internalise it and we have to practise it. I think it has clearly improved in the last decade or so. I would say we are probably one of the most networked governments in the world. We are not just talking about it. This is our competitive advantage. This is something in which we have some inherent advantage, because we are small; everybody knows everybody else. We are a flat organisation and we can move things much more quickly than even much larger countries that have many more layers. In such countries you might have the federal government, provincial governments, central government and so on. So we don't have those kinds of complications. We also don't have the geographical problems associated with large countries. We are very compact. So we can make these things happen. But this is not something that happens naturally, it requires constant attention, it requires the attention of the top leadership and I think we will have to continue to focus on this. I think if we do this well, we will gain the recognition of our counterparts as a government that is going to truly be one of the best in the world.

ENDNOTES

[1] Key installations are establishments vital to our nation for the continuous provision of essential services during a national emergency. Examples

of key instillations include the oil refineries on the Singapore Island of Pulau Bukom.

[2] GSM (Global System for Mobile Communications) is the most widely used standard for mobile telephony systems in the world.

[3] Former Commissioner Singapore Civil Defence Force (SCDF)

[4] A Work Improvement Team (WIT) is a group of people from the same work area irrespective of appointment, who meet regularly to: a) Identify, examine, analyse and solve problems pertaining to their work, b) Help to adapt the work area and hence the department to changing circumstances., c) Discuss and conduct studies on how to improve their working environment, efficiency, quality of service, knowledge and skills, team work, work performance, use of resources, work goals, objectives and targets, systems, methods and procedures. http://www.nus.edu.sg/NUSinfo/WITS/philosophy.htm#Improvement

[5] Also known as the Light Fire Attack Vehicle. This is a formidable vehicle used by SCDF which could maneuver into every corner of a HDB (Housing Development Board) void deck. It is equipped with a hydraulic system for rescue tools, a water mist gun and a water monitor.

[6] Internal Security Department, Ministry of Home Affairs

EDITOR'S NOTES

The Home Team Journal is very privileged to have interviewed Mr. Peter Ho, former Head of the Singapore Civil Service who retired from the Administrative Service in September 2010 after more than 34 years of distinguished service.

While heading the Singapore Civil Service, Mr. Peter Ho was also holding the concurrent posts of Permanent Secretary (Special Duties) in the Prime Minister's Office, Permanent Secretary in the Ministry of Foreign Affairs, and Permanent Secretary for National Security and Intelligence Coordination.

Mr. Peter Ho will continue to contribute to the public sector in various capacities after his retirement. He will serve as a Senior Fellow at the Civil Service College and also as a Senior Advisor to the Centre for Strategic Futures, in which he was instrumental in setting up, to strengthen the capacity of the Singapore Public Service to prepare for the future.

New Media:
Potential Value
for *Home Team Agencies*

MR. KOH KEW SOON

THE QUESTION CAN be stated simply: Why is new media relevant for the Home Team? The answer, however, may require a lot more space, both to state and to elucidate. This article is an attempt to do so, by looking at where new media is heading and the manifold opportunities it offers.

SOCIAL MEDIA: WHAT'S HAPPENING AND WHAT NEXT

Growing Popularity of Social Media in Singapore

THERE IS NO doubt that social media is big, and getting even bigger, not just worldwide but in well-connected Singapore. A recent study by *Nielsen* (Nov 2009) found that 52% of Singaporeans were already using social media[1]. According to *ComScore*, more than 2.5 million people here each spent an average of 21 hours online in Feb 2009, with instant messaging, entertainment, and social networking topping their online activities[2]. *Synovate*'s Young Asians Study (Mar 2009) found 60% of Singaporean youth into blogging, with 35% updating their blogs regularly; while 51% updated their social network profiles as well as read profiles of others[3]. The *Nielsen Media Index* (Oct 2009) found 59% of Singaporean adults going online daily, with Generation Y (aged 15-29) favouring online communications, entertainment and social networking[4].

The top social media platforms here are Facebook, YouTube, Wikipedia, Twitter, and Flickr, each leading its own category[5]. In particular, Facebook has grown tremendously popular and is today Singapore's most visited online destination, even overtaking search engine Google since Aug 2009. Today, 42% of local Internet users, or about 27% of Singaporeans, are Facebook users. There are now more than 2 million Singapore-based Facebook accounts[6]. Twitter, while new, is growing fast with an estimated 89,700 local Twitter users[7].

A Singapore Polytechnic survey (Dec 2009) found that daily, 64% of local youths visited Facebook, 35% YouTube[8].

What's New in New Media

THE NEW MEDIA landscape has continued to develop rapidly, with new technologies and rich applications emerging, underscoring the need to constantly anticipate trends and their impact, so that even if we cannot manage to 'stay ahead of the curve', we can at least stay abreast of it.

Globally, a significant trend in 2009 was the shift towards a '**Real-time Web**', including 'real-time' news, comments, interaction, search, collaboration, etc[9]. While instant messaging, voice-over-Internet and video-conferencing have long catered to smaller groups, the rise of Twitter and Facebook have enabled 'instant' social updates to be sent, shared and forwarded among much larger groups. Third-party sites can also integrate such discussions with other live content such as video streams[10]. Search engines and social news sites have also upgraded themselves to offer more 'real-time' search results, allowing one to search and find news, blog posts, tweets or other content published just minutes ago. A new breed of websites (such as *almost.at*) lets you observe and discuss events happening remotely, in real-time, via a combination of text-based and visual feeds. Mainstream media companies, recognising the potential of 'real-time news' and the need to compete with social media sources, have used Twitter and 'breaking news' sites to deliver more immediate news.

There were more than 450 million **mobile Internet** users worldwide in 2009, a number that is expected to more than double by the end of 2013[11]. In Singapore, the mobile penetration rate increased to 136% in December 2009 from 130% in January 2009[12]. Worldwide, the iPhone alone accounts for about 33% of mobile web traffic[13]. Globally, sales of the iPhone have reached 57 million units, and Singapore is number six on the list of countries using the iPhone. Today, more than three million people in Singapore have mobile 3G subscriptions, allowing them to 'plug into' countless online sites and data while on the move.

At the same time, **geo-spatial** (geo-location) applications have grown more sophisticated and powerful, allowing the integration of richer data, including social and multimedia, with interactive map interfaces. *GoThere.sg*, a popular local start-up, provides dynamic maps with instructions on how to get from A to B using public transport. *Google Street View* allows one to virtually move through any street in Singapore and have a 360^0 horizontal view of each location. Meanwhile, the Singapore Land Authority has

launched *OneMap* to bring combined locational data from government agencies to the public via an online map interface.

Related to mobile and geo-spatial technologies is the rise to **augmented reality**, a hot growth area in the new media landscape. Utilising a range of technologies such as GPS and built-in compasses, it brings location-based data to mobile phone screens, enabling layers of web data or virtual images to be super-imposed on top of 'live' camera views on mobile phone screens. Augmented reality applications such as *Layar* and *Wikitude* are already available locally on iPhones and Android-based phones. Increasingly, as more online data such as videos or tweets become geo-tagged, we will see even richer data and social interaction via mobile devices.

NEW MEDIA OPPORTUNITIES FOR THE HOME TEAM

THIS SECTION WILL include a number of examples of new media usage from overseas agencies, presented as possible opportunities with some observations from the writer. Individual Home Team agencies are in the best position to evaluate whether to explore them conceptually, experiment on a small scale (e.g. a pilot/trial) or perhaps go further, while complying with existing policies and addressing concerns such as security. One should always weigh the potential benefits versus the likely costs involved and possible drawbacks.

Image-Building, Community Outreach and Recruitment

NEW MEDIA, WITH enriched multimedia, interactivity and the potential to form online communities and galvanise positive action, is an ideal platform for image-building, community outreach and recruitment, especially if young Singaporeans are a key target audience.

The use of **multimedia** (online videos and photos) to show-case the actions of uniform groups and security agencies is not new. The challenge is how to make such multimedia content more interesting, appealing and even interactive, in order to capture attention and connect to youths, and have a chance of spreading virally. This requires innovation, and perhaps a degree of humour, originality and spontaneity in line with the online culture.

Internally, this may require more **dedicated resources and roles**, such as setting up a dedicated role or portfolio for digital communication and engagement. For example, the UK's West Midlands Police recently announced that a senior officer, Asst Chief Constable Gordon Scobbie, had taken on a new portfolio for digital engagement[14]. It would also require more extensive use of online

channels to disseminate official communications, such as speeches, press releases, press conference, interviews etc, in a timely manner. Content would also need to be customised and adapted for different online platforms. For example, a long article, like the one you are now reading, is generally ill-suited for online reading.

While not essential and dependent on personal inclinations, it would be useful for **key leaders and spokespersons** to be new media-savvy and to have an active online presence, e.g. a Facebook page or a blog, where the public can read about their vision and hopes for their organisations, and their thoughts on key issues and challenges. They can help to recruit by blogging or posting about their organisation's need for public-spirited individuals with similar interests and dedication to join their team. Recruitment can also be done via a corporate blog. One example is the Houston Police Department, which has a recruitment-dedicated blog[15] with daily entries giving insights into police jobs; specific Facebook and Twitter content on recruitment; an official recruitment site; and on top of all this, the Houston Police Department Chief's own blog.

At the same time, especially for agencies that perform a vital public service, one could consider allowing the **rank-and-file and specialists** to share about their work online (subject to security and other policies), in order to give the public more intimate, rare glimpses into the type of work they do and their thoughts. This can be done using a combination of tools such as blogs, Facebook, Twitter, videos and photos. Videos can feature interviews with front-line staff, or show them going about their daily work. Photos can capture highlights, such as parades, exercises or when forces are deployed in action. While there is no need to over-dramatise the 'action', it would help to show the dynamic nature of the job. Recruitment messages can be woven in as well. The Police Chief in Lincoln, Nebraska, USA, himself an avid blogger, recently got 18 of his police academy recruits to blog about their experience[16].

Where **social networking** is concerned, Facebook is the obvious choice given its overwhelming popularity in Singapore. A good thing about Facebook is that it also allows many parallel channels for reaching out. For example, you can set up an official Facebook fan page for an organisation. But at the same time, individuals in your organisation can also use their personal pages to reach out at an individual level. The individual pages can connect at a more personal level, resembling the "cop on the beat" stopping to chat with any passersby. It is also possible to create social network pages targeted at youths or children, so

that children who are witnesses to or victims of crimes have a safe, friendly online channel to inform or seek help from the police. An example is the "My #1 Friend is a Cop" MySpace page set up by the Fairfield (California) Police Department[17].

Appropriate **online advertising** can also be considered for recruitment or public education. It should be cost-effective to adapt existing print/outdoor ads to new media. Online advertising can be done on selected websites, search engines and social networks. Ads on Google, the leading search engine in Singapore, can be bought for specific search words or phrases, and can be targeted at people logging on from Singapore. For social ads, Facebook is probably the best choice due to its reach; furthermore, one can target specific sub-groups (age, gender and other demographics) among Singapore's Facebook users.

Going further, one can perhaps consider creating a **Facebook app** for existing members of Home Team agencies to recommend job openings to their friends on Facebook. This sort of social recommendation can be more effective than ordinary advertising because the invitation comes from a friend who knows one's preferences and inclinations.

The U.S. Federal Bureau of Investigation (FBI) is a good example of an agency that has actively leveraged on various new media platforms for image-building, outreach and public education. Besides official presences on key social media platforms like Facebook, Twitter, YouTube, and even billboards on Second Life[18], it also created a "Most Wanted" iPhone and iPod Touch application which was downloaded more than 350,000 times in 80 countries worldwide between Feb-May 2009. Among its most successful initiatives is a series of FBI-branded **widgets**[19] that the public can add to any blogs/websites to share its online content more widely. According to the FBI, their widgets have been "enormously popular", and the "first four widgets alone have brought more than 2.5 million people to our website", while the latest widgets averaged "more than a thousand views a day". Their latest (Jan 2010) is a Video Widget[20] that allows users to embed FBI's videos. It comes with a selection of several videos, social sharing options, buttons linking to various FBI social media content, RSS alerts, email alerts, etc.

Video games and online games are another form of digital media that can help to showcase an organisations' work and contributions, and even allow the public a 'hands-on', interactive way of virtually 'sampling' a job and its challenges. For example, a game can simulate how the police patrol and deal with street crimes. Casual games and highly interactive social games on social networks like Facebook are

especially useful, because they are generally cheaper to produce, and can reach more people because they are easy to play, there is no need to download or install and well-designed games can spread virally. It is also possible to consider 'deeper' games such as the CSI games that allow players to immerse themselves in the challenge of solving crimes. Beyond games, one can also tap on 3-D virtual worlds such as Twinnity to host virtual events (e.g. virtual parades or a virtual emergency exercise) or virtual locations, or create interactive online virtual tours of police stations, fire stations, simulated crime scenes and other interesting locations. While a 3-D world presence or 3-D tours may have a novelty appeal, one should also consider the downside as they can be costly to produce and their reach and impact may be limited compared to that of social games.

For all multimedia, games, interactive digital media, widgets etc, it is important to have a clear publicity strategy using efficient online distribution channels/mechanisms to ensure that they have sufficient reach and impact to justify the resources invested in creating them.

Public Education and Alerting

New media is also a useful channel to educate the public, e.g. on personal safety/security and crime prevention. For example, YouTube videos can give step-by-step instructions on matters such as fire safety, while Twitter messages can be used to disseminate daily tips or alerts about crimes/hazards. For more interactivity, a Facebook app or game can guide people through a step-by-step process, while online quizzes/polls can be used to assess their level of knowledge. Online communities can be set up for those with special interest in learning more, sharing with each other, or giving their feedback/suggestions. Hard copy resources like posters and booklets should be digitised as far as possible and made available online, either in PDF or other easily browsable and printable formats. One can also provide links to online resources for further reading.

New media can also be used to **highlight good citizen contributions** and praise public-spirited volunteers, in order to encourage and reinforce such positive behaviour. But sometimes, the reverse can also be useful. Some police forces have adopted an online '**name and shame**' tactic. The Denton Police Department in Dallas, USA, publishes its arrests on Twitter, together with Twitpics showing mugshots of the people arrested[21]. This not only shows that the Police Department is actively doing its job, but also deters potential criminals. In another example, over the 2009 year-end festive period, police in the Housten-area county of

Montgomery decided to name and shame drunk drivers on Twitter[22]. More positively, new media can also highlight rehabilitation and reintegration efforts for convicts, and help ex-convicts gain acceptance and community support. An example is the Yellow Ribbon Project website in Singapore[23].

An **online database** of crime reports is also one way of educating and alerting the public. One example is www.crimereports.com, which not only collates data from many U.S. law enforcement agencies on crimes, but also integrates the data with Google Maps.

In fact, **geo-tagging** has a lot of potential for safety/crime-related education and alerting. All relevant location-based details can be geo-tagged, such as crime scenes or high-risk spots, locations of hazards (e.g. bush fires), locations of police stations/posts and fire stations, locations of nearest life-saving facilities such as first aid boxes or defibrillation kits, etc. Once geo-tagged, such information can be made available on online interactive maps (such as Google Maps or SLA's OneMap) or integrated with other mash-ups and applications. Location-specific content such as videos and photos of locations can also be geo-tagged, so that they will turn up when the public makes location-specific searches, and can also be used with geolocational apps/maps.

There is an established trend of **crime-mapping**. Examples include: *Stumble Safely*[24] (which alerts people on crime spots in Washington so that they can navigate safely though the streets, day or night); and *Oakland Crimespotting*[25] (which maps crime types to different locations and one can view how this changes over time; the site also provides crime reports, information on police beats and alerts via RSS and email). Over at Australia, you can find the *NSW Crime Explorer* and *How Safe is Your Suburb*[26]. Even the media have picked up crime-mapping. For instance, the *LA Times's The Homicide Report*[27] maps homicides to Google Map locations. Various other examples exist[28].

Geo-spatial information can also be **integrated** with other types of content. For instance, YouTube videos of *Crime Watch* episodes can include embedded video links to Google Maps showing the locations of the crimes, with additional information. One can even include the location's street photo from *Google Street View Singapore* to give the public a view of the actual crime scene, without having to physically take a photo of it.

The rising adoption of **mobile devices with geo-tagging features and apps** brings even more opportunities. Geo-tagging can allow Singaporeans with smart phones to assess location-specific information on the go, to better prepare them

for threats or eventualities. This can further extend into **augmented reality** mobile applications; for instance, apps that tell people which direction to go, how to get to, how far to travel or how long it would take, to reach the nearest police post. Or imagine a mobile application that triggers whenever one walks past a crime scene, popping a photo of a suspect and inviting witnesses to provide information. Augmented reality can also be used in conjunction with crime scenes[29].

Citizen Alerting and Reporting

A KEY COMPONENT OF Web 2.0 is the rise in user-generated content and 'citizen journalism'. The example of SPH's STOMP website shows there is no shortage of Singaporeans keen to contribute. STOMP's most popular section is the "Singapore Seen" section where users submit photos or videos highlighting mainly municipal issues.

In the same manner, new media can be used to encourage active citizenry through positive reporting and alerting of crimes or safety threats/incidents. Camera-equipped mobile phones make it easy for the public to not just report an incident or threat immediately, but to also **record photos or videos** and **send them to the relevant authorities** (via MMS, websites or apps), to provide more concrete evidence and information. Additionally, the contributor can **geo-tag** this information so that the authorities can ascertain the precise location for follow-up. Responders to all kinds of emergency situations can glean valuable information from videos/photos before they even arrive at the scene.

Mobile apps can encourage the public to help keep a watchful eye on potential repeat offenders and to alert vulnerable individuals. An example is the *Offender Locator* iPhone app that reveals the location of sex offenders, reportedly downloaded more than a million times[30]. Mobile apps can also allow the public to not just report a crime in progress but also seek immediate assistance, including practical tips on what to do to protect themselves. For instance, the *Jtrek* app allows one to quickly alert friends, families and security personnel of an emergency or a crime in progress[31].

Facebook can also be a good platform for citizen reporting, and SPF has already been doing so to some extent. It has even caught the notice of a law enforcement blogger who praised the SPF's Facebook fan page as an example of progressive use of social media for law enforcement[32]. Beyond just using a Facebook fan page, one can even create a Facebook app to facilitate reporting. For example, the Greater Manchester Police created a

Facebook app (GMP Updates) that provides users with crime news and missing-persons stories while making appeals for information. Various U.S. police departments are also using Facebook as a tool to fight crime, including departments in Greenland (Indiana), Salinas (California), Shelby (Ohio), Gainsville (Florida), Chicago, Dallas, etc[33].

Finally, **dedicated neighbourhood portals** can also enable residents to interact with Home Team agencies and to exchange information with them. Portals that cover specific neighbourhoods are useful because, again using the example of Police, relevant Police Divisions or police officers manning posts or patrolling in a neighbourhood can interact directly with the residents in that neighbourhood. This will enable more direct and focussed sharing of information and alerts. An overseas example is Nixle[34], which provides a one-stop portal for sharing and finding information relating to a specific community. An advantage over social media is that information on such a portal can be more secure and identity-certified/authenticated, thus providing a trusted online channel for "local, county and state law enforcement and government agencies to connect with local residents over cell phone, email and web and to deliver information"[35]. In addition, Nixle is integrated with Twitter, allowing citizens to easily interact and give feedback via Twitter[36].

Crisis Communications and Management

While new media is useful for both *sudden crises* (e.g. civil disasters, terrorist attacks) and *creeping crises* (e.g. pandemics), it is especially important for the former because demand for information is likely to spike tremendously in the immediate aftermath. **People will be searching online** for details (who/what/where/when/how) and expect to find updates, advisories and assurances from the authorities. But instead of visiting government websites, many may simply do an online search and trust the search engine to lead them to relevant sources. Others will turn to specific platforms to satisfy specific information needs; such as Wikipedia for factual details; YouTube and Flickr for multimedia; Twitter for blow-by-blow updates; and Facebook and discussion forums for online views. Hence, a key challenge for the authorities is how to leverage on these platforms on top of official websites.

With the move towards **real-time media** (i.e. from new media to 'now media'), people will expect to find up-to-date information very quickly. So another key challenge is for the authorities to speed up internal processes and reduce response time

in order to quickly generate and push out information through online channels. This would require thorough preparation and planning during 'peacetime', to lay the groundwork for the use of various new media channels, and to prepare relevant new media content and 'templates' as far as possible. In short, it is best to **proactively pre-empt and prepare**, rather than be reactive.

The U.S. Federal Emergency Management Agency (FEMA) is an example of an organisation that has made use of new media platforms during both peacetime and crises. Its comprehensive website includes a full, searchable media library (videos, photos and audio files), various emergency preparedness widgets for downloading, and a detailed list of RSS feeds for different topics and regions[37]. This is complemented by accounts on YouTube, Facebook and Twitter that are regularly updated on preparedness, protection, response, recovery and mitigation efforts. Recently, there is news that FEMA is searching for a social media company that can provide on-demand services to deliver information from disaster areas via social media channels[38].

During a crisis, **emergency messages and alerts** can be pushed to recipients via various channels. An example is the Arizona State University's use of a Facebook app, Twitter and RSS to complement email and text messaging[39]. These are integrated into a single emergency messaging system for broadcasting messages. In Singapore's context, Facebook can be especially useful in providing emergency alerts, since a significant segment of the local population is on Facebook, and can also access it using mobile devices.

Going beyond Government communications, new media can also be used for **sharing of data** between responders, rescue workers, volunteers, hospitals, charity/humanitarian organisations and members of the public, in order to facilitate crisis rescue/recovery efforts, to help the public. Also, community resilience can be strengthened by having online platforms and channels where the general public can chip in to give their support in various ways (e.g. by volunteering or providing asset, monetary or emotional support).

Take the recent **Haiti earthquake**. In its aftermath, while little was done by the Haiti government, the international community used a number of digital platforms to help Haitians and rescuers[40]. Open-source maps and geolocational data were shared via platforms like *Haiti OpenStreetMap*[41], providing locations of critical infrastructure, damage buildings, health facilities, etc. Many of these maps were also available via mobile apps so that responders and rescuers could assess them anywhere in or outside Haiti[42]. A website,

wehaveweneed.org[43], was set up so that donors could quickly match available resources with the victims' needs (food, fuel, medical, shelter, transport, etc). A *Person Finder app*[44] helped people to share and find information on people. The *Help Haiti Heal* website[45] allowed people to check on the status and locations of hospitals and to find food, water, shelter and other resources. The *Relief Oversight website*[46] tracked how disaster relief organisations were allocating donated resources in Haiti, ensuring they were properly utilised. A *Hatian Voices* websites enabled the Haitian survivors to tell their stories.

At the same time, there was much activity on social media platforms. An entry on the earthquake was quickly started on Wikipedia and the public contributed thousands of edits, adding details, photos, citations, descriptions, etc. Two key Facebook groups were created ("Earthquake Haiti" and "Support the Victims of The Earthquake in Haiti") with several hundred thousand members. More than 36,000 videos relating to the earthquake were uploaded to YouTube, including raw news stories, footage of the earthquake and rescue efforts, and celebrities calling for donations; while Flickr carried more than 10,000 photos. Haiti-related topics such as "Help Haiti" and "Port-au-Prince" also dominated Twitter discussions. Relief and charity organisations such as the Red Cross, Yele Haiti and UNICEF also used a range of social media platforms to call for donations. Various social media giants also chipped in, with Google making post-earthquake images available on Google Earth; YouTube adding ticker-tape messages on every page to call for donations; Facebook adding information to its global relief and disaster relief pages; and even Zynga, the leading producer of Facebook games, allowed its players to donate directly from within games.

The Haiti example shows the range of uses of new media for managing crises. We can perhaps sum it up with a few C's: (1) ***Communicate*** – for the authorities to communicate key messages and information to key audiences; (2) ***Coordinate*** – for responders, rescuers, volunteers and relief organisations to coordinate efforts; (3) ***Connect*** – for people to locate missing friends/relatives; (4) ***Charity*** – to solicit and enable donations; (5) ***Comfort*** – to help the community provide emotional and psychological support. While such C's are often initiated ground-up, government agencies can also play a role in catalysing or supporting them, if not initiating them.

A final point is the need for **innovation**. Twitter, with its mobile-friendly nature, was a useful tool for everyone in Haiti to exchange news and information on the go, but is limited to 140 characters per tweet.

To enable more information to be packed in and more precise targeting, the community invented a new hashtag syntax[47] with very specific hashtags. For example, hashtags such as #need or #injured could be used to trigger a need for help, while #name, #loc and #contact provided valuable information for finding and contacting people.

CONCLUSION

While new media has brought many opportunities, it has also brought **new challenges**. These include the battle for eye-balls as online sources continue to proliferate; the ever-rising challenge of online monitoring and horizon scanning; the need to deal with online rumours and misinformation; the need to authenticate one's own information; and the need to adapt internal processes to the 24/7, real-time nature of new media. For law enforcement agencies in particular, two additional challenges are: balancing the need for IT security against the need for access to new media technologies and platforms; and the use of new media by criminals[48] and terrorists.

To deal with these challenges, and to leverage on the many opportunities, **there is no easy short-cut**. Public sector agencies must build up their internal new media capabilities and experience; allocate more resources; continually experiment and innovate with new tools and initiatives in new media communications; be familiar with the latest platforms and tools; and learn to apply the best practices for them. Agencies must also develop a clear new media strategy, bolstered by clear standards and internal guidelines and procedures[49].

> "New media is just a vessel. There is no substitute for good content."

It is also important to **align new media strategies with one's overall communications strategy** for any issue or subject matter. New media is just a vessel. There is no substitute for good content. Online communications must also be balanced and integrated with offline communications.

A final point – **don't do it alone**. New media works best as a community effort. Tie up with fellow agencies. Better still, tie up with the public. Form partnerships with the private and people sectors and, where appropriate, leverage on the online community for crowd-sourcing and third party advocacy. Invite the public to contribute feedback to user-generated-content, but also be prepared to engage them online when necessary.

REFERENCES

1 ChannelNewsAsia (3 Feb 2010) "Social media part of life in S'pore, especially among the young: Nielsen" http://www.channelnewsasia.com/stories/singaporelocalnews/view/1034867/1/.html

2 ComScore (27 Mar 2009) "Singapore Internet Users Spend Half of Online Time on Social and Entertainment Sites" Singapore Internet Users Spend Half of Online Time on Social and Entertainment Sites

3 Media.asia (25 Mar 2009) **"Synovate shows young Asians are driven by media and music"** http://www.synovate.com/news/article/2009/03/synovate-survey-shows-that-young-asians-are-driven-by-media-and-music.html

4 Nielsen (23 Oct 09) **"Popularity of Social Media and the Internet Continue to Rise in Singapore"** http://www.acnielsen.com.sg/site/20091023.htm

5 According to web traffic tracker Hitwise, whose data is based on local ISP traffic

6 Based on *Facebook Ads*, which estimates the number of Facebook accounts tied to each country. Some people may have multiple accounts.

7 Sysomos (Jan 2010) **"Exploring the use of Twitter around the world"** http://blog.sysomos.com/2010/01/14/exploring-the-use-of-twitter-around-the-world

8 938live.sg (8 Dec 2009) **"Survey shows half of youths spend over 3 hours daily surfing net"** http://www.938live.sg/News/Singapore/EDC091208-0000318/Survey_shows_half_of_youths_spend_over_3_hours_daily_surfing_net

9 CNN.com (10 Dec 2009) **"Brace yourself for the real-time Web"** http://www.cnn.com/2009/TECH/12/10/cashmore.realtime.web/index.html

10 This was demonstrated by a highly successful CNN-Facebook collaboration covering U.S. President Obama's inauguration in early 2009. In the local context, ChannelNewsAsia featured a Facebook Livestream integrated with live streaming video for PM's National Day Rally 2009.

11 IDC (9 Dec 2009) **"Number of Mobile Devices Accessing the Internet Expected to Surpass One Billion by 2013"** http://www.idc.com/getdoc.jsp?containerId=prUS22110509

12 From IDA **"Statistics on Telecom Services for 2009 (Jul – Dec)"** http://www.ida.gov.sg/Publications/20070618184449.aspx

13 Read Write Web (11 Dec 2009) **"10 Ways Social Media Will Change in 2010"** http://www.readwriteweb.com/archives/10_ways_social_media_will_change_in_2010.php

14 (5 Jan 2010) **"New Twitter and Facebook Role for Senior West Midlands Officer"** http://www.west-midlands.police.uk/latest-news/press-release.asp?id=1640

15 http://www.hpdblog.com

16 (30 Jan 2010) **"Recruits Who Blog"** http://connectedcops.net/?p=1523

17 (5 May 2009) **"In Fairfield, California, My #1 Friend is a Cop"** http://cops2point0.com/2009/05/05/case-study-in-fairfield-california-my-1-friend-is-a-cop/

18 (5 May 2009) http://www.fbi.gov/page2/may09/socialmedia_051509.html Also see: TechCrunch, 15 May 2009 **"FBI Adds Facebook, YouTube, Twitter Profiles. MySpace Completely Dissed"** http://techcrunch.com/2009/05/15/fbi-adds-facebook-youtube-twitter-profiles-myspace-completely-dissed

19 http://www.fbi.gov/widgets.htm

20 TechCrunch (8 Jan 2010) **"The FBI Adds New Widgets And Facebook Quizzes To Its Social Media Arsenal"** http://techcrunch.com/2010/01/08/fbi-widgets-facebook-quiz/

21 Cnet News (18 Apr 2009) **"The city where every arrest gets twittered"** http://news.cnet.com/8301-17852_3-10222755-71.html?tag=mncol;txt

22 "Cnet News (26 Dec 2009) **"Police to put drunk drivers' names on Twitter"** http://news.cnet.com/8301-17852_3-10422062-71.html

23 http://www.yellowribbon.org.sg

24 http://outsideindc.com/stumblesafely

25 http://oakland.crimespotting.org/map Read more here: http://mike.teczno.com/notes/oakland-crime-maps/VI.html

26 http://googlemapsmania.blogspot.com/2009/12/google-maps-of-australian-crime.html

27 http://projects.latimes.com/homicide-report/blog/page/1/

28 See, for example, those listed at http://www.programmableweb.com/tag/crime.

29 Kjetil Sandwik and Anne Marit Waade **"Crime Scene as Augmented Reality On Screen, Online and Offline"** http://www.krimiforsk.aau.dk/awpaper/KSAWcrimesceneas.w5.pdf

30 CNN.com (30 Sep 2009) **"iPhone apps help track sex offenders, spot crime"**

http://www.cnn.com/2009/CRIME/09/29/iphone.app.fight.crime

31 www.redorbit.com (22 Jan 2010) **"JTrek Smartphone Personal Security App Downloaded More Than 5000 Times During Consumer Electronics Show 'CES 2010' Week"** http://www.redorbit.com/news/technology/1812965/jtrek_smartphone_personal_security_app_downloaded_more_than_5000_times/index.html?source=r_technology

32 http://michaelvallez.com/2009/10/facebook-slowely-becoming-law-enforcement-tool

33 www.insidefacebook.com (19 Feb 2010) **"Police Use Facebook to Fight Crime, Talk to Residents"** http://www.insidefacebook.com/2010/02/19/police-use-facebook-to-fight-crime-talk-to-residents Also, read: http://info.dailysplice.com/blog/best-ways-police-use-social-media for more examples.

34 http://www.nixle.com

35 http://en.wikipedia.org/wiki/Nixle

36 Cops2point0.com (12 May 2009) **"Nixle Adds Stability to Tyrone, GA Tweets"** http://cops2point0.com/2009/05/12/nixle-adds-stability-to-tyrone-ga-tweets

37 FEMA website: http://www.fema.gov; Media Library: http://www.fema.gov/medialibrary; Widgets: http://www.fema.gov/help/widgets; RSS feeds: http://www.fema.gov/help/rss.shtm . Also see this FEMA press release (2 Nov 2009) on its social media efforts: http://www.fema.gov/news/newsrelease.fema?id=49302.

38 http://washingtontechnology.com/articles/2010/02/12/fema-social-media.aspx

39 (12 Feb 2010) "Arizona State Adds Facebook and Twitter for Emergency Alerts" http://campustechnology.com/articles/2010/02/12/arizona-state-adds-facebook-and-twitter-for-emergency-alerts.aspx

40 Gadgetwise (27 Jan 2010) **"Digital Help for Haiti"** http://gadgetwise.blogs.nytimes.com/2010/01/27/digital-help-for-haiti

41 http://crisiscommons.org/Haiti-Open-Street-Map

42 http://wiki.openstreetmap.org/wiki/WikiProject_Haiti/Earthquake_map_resources

43 http://wehaveweneed.org

44 http://haiticrisis.appspot.com

45 http://helphaitiheal.wordpress.com

46 http://www.reliefoversight.org

47 ReadWriteWeb (19 Jan 2010) **"New Twitter Hashtag Syntax for Sharing Information During Catastrophes"** http://www.readwriteweb.com/archives/a_new_twitter_hashtag_syntax_to_help_during_catast.php

48 Well, aside from the occasional helpful criminal like: Mashable (13 Jan 2010) **"Criminal Taunts Police on Facebook, Gets Caught"** http://mashable.com/2010/01/13/facebook-criminal

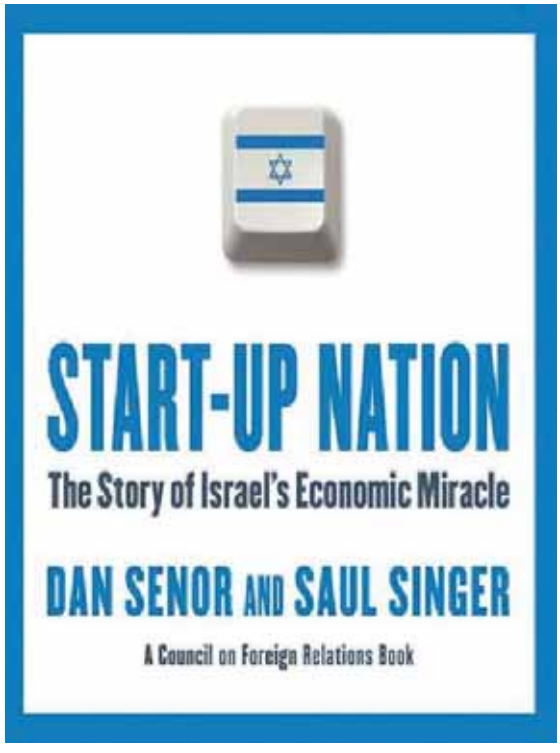
49 Public sector agencies can refer to the restricted document "Social Media Guidelines for Government Communications" distributed by MICA in Feb 2010. Do note, however, that these are just general tips, and one must always be flexible in adapting them to the situation at hand.

EDITOR'S NOTES

Mr. Koh Kew Soon is the Deputy Director leading the New Media Unit at the Ministry of Information, Communications and the Arts (MICA). He was an Information Officer with MICA for about 12 years, during which he was involved in various government websites and online initiatives. He has also delivered a well-received lecture at the Ministry of Home Affairs Headquarters in September 2009 at a seminar on New Social Media organised by the Media Studies Unit of MHQ/MHA. His current work includes new media research, capability building and providing support to government agencies.

Book *Review*: Start-up Nation

the Story of Israel's Economic Miracle



Start-Up Nation:
The Story of Israel's Economic Miracle.
By Dan Senor and Saul Singer.
New York: Twelve, 2009. 320 pp.

SUSAN SIM
Adjunct Lecturer, Home Team Academy
& Consulting Editor, Home Team Journal

Soon after the 2006 Lebanon War, with damage from 2,000 missile strikes still visible, first Bill Gates, then Warren Buffett, showed up in Israel. The richest man in the world was on his first visit to Israel to see why his competitor Google had just opened its second research facility in Israel in a year. The second-richest man in the world was visiting the first company he had ever bought outside the United States.

Buffett, the apostle of risk aversion, was not indifferent to Israel's vulnerabilities when he decided to buy machine tool company Iscar for US$4.5 billion in 2006, authors Dan Senor and Paul Singer tell us. Iscar's main factory and R&D facilities in the northern part of Israeli, eight miles from the Lebanese border, were then, and remain, a prime target for rocket fire. But missiles do not represent catastrophic risk for

Buffett because the plant does not represent the value of the company. "It is the talent of the employees and management, the international base of loyal customers, and the brand that constitute Iscar's value," *Start-Up Nation* quotes Buffett biographer Alice Schroeder as explaining.

What Senor and Singer call the Buffett Test – a company's ability to deliver under adverse conditions – was soon aced by Iscar, whose chairman Eitan Wertheimer decided his factory would not miss a single shipment. "For our customers around the world, there was no war," he recounts for the authors.

It is a familiar story of chutzpah; that blend of gall, brazen nerve, presumption and arrogance often associated with Israelis and Jews in general. In 1991, when Saddam Hussein rained Scud missiles on Israel, Intel's Haifa design centre astounded their American counterparts by staying open and delivering on schedule the 386 chip, then Intel's most important microchip powering most PCs globally. Open in defiance of government orders, Intel Israel created its own "new normal." Carrying gas masks, workers set up a wartime kindergarten on the premises since schools were closed. The more brazen the Iraqi attacks, the larger the staff turnout.

It is this "Israeli grit" – the drive to succeed that is as much national as personal – that allows Israeli start-ups to transcend their geopolitical realities, where war is no impediment to doing business. How else to explain why Israel's foreign direct investment tripled from 2000 to 2005 at a time when Israeli society was being devastated by a relentless string of suicide bombings, say Senor and Singer. They offer more staggering statistics:

Israel has more high-tech start-ups per capita than any other nation on earth; in 2009, the country of 7 million had 3,850 start-ups, one for every 1,844 Israelis. There are more Israeli companies listed on NASDAQ than all companies from Europe and Asia combined. Between 1980 and 2000, Israelis registered 7,652 patents, more than the entire Middle East. In 2008, per capita venture capital investments in Israel were 2.5 times greater than in the United States, more than 30 times greater than in Europe, 80 times greater than in China, and 350 times greater than in India.

How did Israel become such an entrepreneurial hotspot? As *Start-Up Nation* points out with breathless wonder, "almost half of the world's top technology companies have bought start-ups or opened research and development centres in Israel."

With stirring stories of perseverance and success, the book posits that Israel has a culture of innovation that thrives because it has an ecosystem that turns the "unique

combinations of audacity, creativity, and drive" inherent in the Israeli national character into battle-hardened entrepreneurship, helped along in the early years by an interventionist government that was trusted because "at no point did anyone pocket even one cent," and an open immigration policy allowing Jews from anywhere to settle in Israel.

Start-Up Nation often reads like it was co-written with the mothers of an award-winning cheerleading squad, so eager is it to discover the spirit of *davka* residing in every Israeli entrepreneur who succeeded in defying the odds. *Davka*, as Senor and Singer tell us, is "an untranslatable Hebrew word that means 'despite' with a 'rub their nose in it' twist." That Israel has become the strongest economy in the Middle East despite the Arab boycott is sweet revenge.

Where the book gets really interesting is its description of how the Israeli Defense Forces (IDF) has become the incubator of the country's tech-savvy. The millions of dollars that the Israeli military has poured into defence research and training has fostered not only an innovation-is-survival mentality and anti-hierarchical and enterprising ethos, but conscription has also spawned networks of war buddies who feed off each other's creativity and connections to create an innovation cluster with a reputation for technology mashups, reaching across different fields and meshing technologies to create entirely new products. Thus the sophisticated electro-optical devices invented by an IDF weapons developer to help a missile hit its target has been transformed by a Israeli start-up into a camera within a pill – the PillCam - that can transmit images from inside your intestines.

Are the ingredients for a successful start-up nation present in Singapore? The national experiences of Israel and Singapore are not too different. Struggle for independence? Check. Compulsory military service? Check. A military reliant on reservists? Check. Living under threat? Check. Government policies to provide financial support for new companies? Check.

So why has Singapore failed to incubate start-ups? Because it is too tidy, too orderly and its people too obedient, say Senor and Singer. "Its growth story notwithstanding, Singapore leaders have failed to keep up in a world that puts a high premium on a trio of attributes historically alien to Singapore's culture: initiative, risk-taking, and agility." Some chaos, including acceptance of "constructive failures," is important because entrepreneurialism requires fluidity. According to a new school of economics, when people can cross boundaries, turn societal norms upside down, and agitate in a free-market economy, radical ideas are

catalysed. "The most formidable obstacle to fluidity is order," *Start-Up Nation* declares.

Most readers can sympathise with their perceptions of Singapore but their analysis of our business culture is glib and dated. We remain orderly and not so tolerant of failure but there is now a new looseness in Singapore that has come with a deliberate open door policy. A premium is now put on risk-taking, even within the public service, and the ranks of self-starter entrepreneurs trying to grow regional wings are growing. In the last few years, there has been a burst of creativity that has attracted Silicon Valley and Japanese conglomerates; often foreign investors have to compete with a slew of government venture capital funds which offer seed money to young start-ups in Singapore.

It may take a few more generations before we produce a Bill Gates. Meanwhile, even within the Home Team, technopreneurs are emerging. Read the Singapore Police's Innovation Journal. Not only are our police units tying up with local start-ups to blend new and existing technologies to create crime prevention tools such as WaveSecure, a system to enable recovery of lost cell phones and protect confidential information, but our boys in blue are also designing ingenious solutions to work problems, such as the submersible inspection device, a PVC pipe with LEDs that when inserted into a barrel can illuminate its entire contents. A Police Coast Guard team came up with this award-winning innovation to deal with the problem of checking live seafood cargoes kept in water barrels for contraband. The Singapore Civil Defence Force's Red Rhino is another creative solution to the problem of fighting fires in densely built-up areas.

Where perhaps the Home Team has lagged behind is in commercialising its ideas; the focus has been on sharing innovative ideas across the Home Team and the government sector rather than on protecting its intellectual property rights. That too is changing. For instance, the SPF has begun patenting its inventions, such as the Arms Tray, a portable platform for storing all the equipment an officer needs on duty. With this mental shift from treating innovation as creative problem solving to an entrepreneurial activity, the Home Team too could become an incubator of homefront security start-ups in time.

One of the enviable lessons that one takes away from reading *Start-Up Nation* is the idea of "profitable patriotism." Senor and Singer describe several Israeli start-up millionaires who see it their duty to grow new industry sectors in Israel and sustain others through dry spells. The concept of profitable patriotism is not new; during the financial crisis of 1907, banker JP Morgan committed some

of his own money to stabilise the US economy and organised the financial community to join in the rescue.

The excesses of Wall Street have generally overtaken such patriotism impulses. And as *Start-Up Nation* tells us, business clusters mandated by government fiat, such as Dubai's Internet City, Healthcare City, Biotechnology and Research Park et al, have only one main competitive advantage – price. They do not have the tight-knit communities with the emotional commitment and sense of rootedness that are indispensable to sustainable growth. And "some other country will always come along to do it more cheaply."

In resource-constrained Singapore, some other country can always beat us on price. But precisely because of our orderliness – which has come to be equated with efficiency in the business world – the Singapore brand sells. Israel might have guardian angels who pitch to foreign investors as a nation. But ironically, although the Israeli tech start-up that *Start-Up Nation* opens with – Better Place, the electric vehicle services provider – is now on the cusp of commercial success, having just begun its first trial run in Tokyo[1], it is identified as a "California-based" firm in media reports. Even firms with chutzpah cannot always succeed with an Israeli identity.

ENDNOTES

[1] International Herald Tribune, "3 Electric Cabs begin 30-day trial that could lead to expansion," 27 April 2010.

Start-Up Nation is available at the Home Team Library and National Library Board branches.

A publication of the
Home Team Academy

About the Home Team Academy

The Home Team Academy (HTA) is a Department under the Ministry of Home Affairs that is committed to the training of Home Team officers in Homefront Security and Safety. The Academy aims to spearhead training in Counter-Terrorism, Law Enforcement, Crisis Management and Emergency Preparedness. It also conducts a wide range of programmes, including Behavioural Sciences and Leadership Development.

www.hta.gov.sg
ISSN: 2010-0167