# VIEWPOINT: Singapore Aims for Enhanced Information Awareness with RAHS

## *Cross-silo collaboration aims to overcome the complexity and uncertainty of today's threat environment*

## *Strategic Insights*, Volume VI, Issue 3 (May 2007)

by Barry Zellen



## Introduction

The post-cold war world—and in particular, the *post-9/11* world—has evolved into an unexpectedly dangerous place full of hidden dangers and its own strategic surprises. With seemingly unforeseeable—or at least *unforeseen*—and unexpectedly swift lethality, external strategic shocks can still strike from beyond the horizon.

Today's primary danger lies not in the nuclear overkill that held much of the world hostage during the cold war, but in the world's increasing complexity and interconnectedness. And yet, this danger—looming just beyond the horizon of our strategic awareness—curiously enough provides its very own antidote: with enough compute power and a willingness to break down the traditional 'silos' that prevent analysts from connecting the dots and communicating emergent trends to decisionmakers in time to take preventive or preemptive action, we can—in theory—push back the horizon of strategic awareness, enabling earlier detection of strategic threats.

While we may never be able to predict the future with crystal-ball clarity, we can—by fostering greater collaboration among the gatekeepers of our strategic intelligence, and integrating hitherto 'stovepiped' pools of classified data with the vast reservoir of open source data—widen the footprint of what's knowable and seeable, so we'll get earlier warning of emerging threats to our national existence.

As explained by Ambassador Barry Desker, Dean of the S. Rajaratnam School of International Studies at Singapore's Nanyang Technological University in his opening remarks to the International Risk Assessment and Horizon Scanning Symposium held in Singapore in March 2007, "Today, the current threat environment is marked by complexity and uncertainty. Thanks to what the journalist Tom Friedman calls the 'democratizations' of finance, information and technology, many nations are becoming increasingly vulnerable to a range of asymmetric threats such as transnational terrorism, financial shocks, pandemics and supply chain fragility."

The United States recognized this in those fiery moments of strategic shock following the 9/11 attacks, and sought to remedy the solution with the briefly lived Total Information Awareness (TIA)

program, and its Information Awareness Office (IAO), conceived by the Defense Advanced Research Projects Agency (DARPA). According to the online encyclopedia *Wikipedia*, the IAO was established in January 2002 “to bring together several DARPA projects focused on applying information technology to counter transnational threats to national security.” IAO’s mission was defined to “imagine, develop, apply, integrate, demonstrate and transition information technologies, components and prototype, closed-loop, information systems that will counter asymmetric threats by achieving total information awareness,” and its research “was conducted along five major investigative paths: secure collaboration problem solving; structured discovery; link and group understanding; context aware visualization; and decision making with corporate memory.”

But a strong backlash among the American public, fearful of the potential erosion of civil liberties, led the U.S. Congress to defund the TIA program less than two years after it was established. As *Wikipedia* explained, “Following public criticism that the development and deployment of these technologies could potentially lead to a mass surveillance system, the IAO was defunded by Congress in 2003, although several of the projects run under IAO have continued under different funding… several TIA projects continued to be funded under the classified annexes to the Defense and the Intelligence appropriation bills in 2003 and subsequently,” and “an unknown number of TIA's functions have been merged under the codename ‘Topsail’.”

Ironically, the very mission of TIA that was defunded by the U.S. Congress was echoed in the recommendations of the bipartisan *9/11 Commission Report* issued in July 2004, a year after the TIA project was mothballed. TIA had been created to address the very information issues that the *9/11 Commission* concluded were responsible for America’s failure to predict the 9/11 attacks, and which—with the proper processes and information systems in place—could have been prevented.

According to the *9/11 Commission Report* ("Unity of Effort: Sharing Information," pp. 24-25), "The U.S. government has access to a vast amount of information. But it has a weak system for processing and using what it has. The system of 'need to know' should be replaced by a system of 'need to share.'" Accordingly, the 9/11 Commission recommended that “the President should lead a government-wide effort to bring the major national security institutions into the information revolution, turning a mainframe system into a decentralized network,” adding that “the obstacles are not technological. Official after official has urged us to call attention to problems with the unglamorous ‘back office’ side of government operations.” The 9/11 Commission further explained that “no agency can solve the problems on its own—to build the network requires an effort that transcends old divides, solving common legal and policy issues in ways that can help officials know what they can and cannot do. Again, in tackling information issues, America needs unity of effort.”

9,660 miles from the Washington, where the internecine politics inside the Beltway are but a distant curiosity, the government of Singapore recognized the strategic importance of developing the very same type of collaborative information systems envisioned by the authors of the *9/11 Commission Report* and by DARPA in the days and weeks following the 9/11 attacks. Indeed, on July 20, 2004—just two days before the 9/11 Commission released the public version of its report—the government of Singapore introduced its new *Strategic Framework for National Security*.

According to the website of Singapore’s National Security Coordination Centre (NSCC), Singapore has recognized that “as transnational terrorism had transformed the national security landscape, we could no longer deal with it in the traditional stove pipe manner” and “to cope with the new security challenges, we needed to deal with current security threats on a 'whole-of-government' basis instead of dividing the tasks into watertight compartments to be dealt with by separate ministries, as was done in the past.” On July 20, 2004, Singapore’s Deputy Prime Minister (DPM), Dr Tony Tan, “laid out the case for a new strategic framework on national

security in Parliament. The *Strategic Framework for National Security* aimed to address the issues and close the gaps which we had identified and put in place the machinery to enable the Government to systemically deal with the security issues confronting our nation… When DPM Tan stepped down on 31 Aug 05, the NSCC came under DPM Professor S. Jayakumar, who was concurrently appointed Coordinating Minister for National Security."

Among the three core groups within the NSCC are the Policy Group, the Strategic Planning Group, and the Risk Assessment and Horizon Scanning Group; it's the latter group, known as RAHS, that is tasked with the mission of transforming the culture of data analysis from stovepipes to collaboration, and integrating new information systems and analytical methods to see beyond the horizon, increasing the predictive power and early warning capabilities of Singapore's traditionally stovepiped government agencies.

As Ambassador Desker explained, "Given the kind of multidimensional challenges that states face today, leaders and decisions makers require actionable knowledge to operate effectively in a complex international environment. They must be prepared to meet a range of conventional and asymmetric threats." He added that "frankly, this task will not be easy," and recalled that "one of the most recurrent aspects of human history is the persistence of strategic surprises such as Pearl Harbor, 9/11 and the SARS crisis." He believes the "roots of these intelligence failures are almost always the lack of information sharing amongst government agencies, or what is commonly referred to as 'stove-piping' or 'silos' as well as rigid mindsets within societies that can only parochially perceive information from one fixed frame of cognitive lenses." In our complex and connected world, he has found "one thing is clear: the traditional responses and mechanisms of national intelligence and security agencies are not enough."

Hence the development of RAHS, which "as envisioned in the Singapore context, encompasses a unique combination of cutting edge concepts, methodologies and technological solutions, and aims to provide policymakers with anticipatory knowledge of the nature of potential upcoming issues so that risks may be minimized and opportunities maximized." Desker explained how "by detecting 'faint' signals; networking and linking the various governmental and private agencies; and fostering shared and informed analysis based on methodological diversity, it is envisaged that RAHS will empower people with greater foresight to minimize the possibility of strategic surprises."

Deputy PM Jayakumar, who serves as Coordinating Minister for National Security and Minister for Law, told attendees of the International RAHS Symposium in Singapore that while "governments are not endowed with any special gift of foresight" and "while we cannot predict the future, we can develop more intelligent systems and robust processes towards monitoring new strategic trends and developments in order to anticipate a diversity of possible outcomes." He noted that "this is not meant to accurately predict discrete events at a particular time and place in the future, but the capability to anticipate general trends and emerging patterns that may take hold in the future." RAHS thus aims to develop "a process that would help uncover elements in the environment not obvious from the start, which could be missed by dependence on one particular approach or a reliance on just one strategic planning tool."

To illustrate both the problem and the solution, DPM Jayakumar recalled how during the 2003 SARS crisis, "Singapore started to receive reports of patients with viral pneumonia in March 2003," but while there had been "were weak signals like open source reports in February which were already pointing to a mysterious lung virus in southern China that had stricken 305 people and killed five," the dots remained unconnected, largely because "there was no apparent context or pattern against which analysts could make inferences." He believes that the RAHS system will "help draw the disparate pieces of information together to alert analysts to potential crisis situations."

At its current stage of development, RAHS is not a panacea for mitigating the risks and dangers

presented by unknown strategic surprises looming over the horizon. But, as Deputy PM Jayakumar explained, “as the RAHS program breaks new ground, our understanding of what works best in our particular context will improve,” and “as such, RAHS is a long-term commitment as well as an R&D enterprise that will evolve over time.” RAHS “already has, and will continue to show promise in connecting silos, challenging mindsets, and developing a ‘need-to-share’ instinct… in contrast to the ‘need-to-know’ mindset, where departments safeguard information within agency silos… For us, the value of RAHS is clear. It has the potential to be a strategic planning process, to facilitate agency collaboration, and to put in place a whole-of-government framework to think about a complex and uncertain future.”