saferCITIES

Brought to you by **NEC**

TECHNOLOGY OUTLOOK FOR 2012

Opportunities to better secure urban environments

OPEN THE DATA FLOODGATES

The role of ICT in fighting floods in Thailand

INTER-AGENCY COLLABORATION

Unleashing the potential of big data

www.futuregov.asia

Safety with a human touch

NEC focuses on enhancing people's quality of life in a world growing more interconnected every day. Through leading IT and network expertise, NEC provides advanced public safety solutions — including innovative multi-biometric, access control and video surveillance systems — that effectively safeguard people in their everyday lives. Driven by its global vision to foster the well being of communities, NEC is committed to providing optimized solutions through its regional specialists. Elevate public safety with NEC.

Learn how you can partner with NEC **www.nec.com**/security

Empowered by Innovation NEC

CONTENTS

saferCITIES

Special Supplement March 2012
www.futuregov.asia

MICA (P) 013/05/2009 • ISSN 2010-0582

Safer Cities is a FutureGov supplement published and distributed free to government, education and healthcare administrators in Asia Pacific. Our mission is to contribute to the development of better governance in the region by providing a unique forum for officials, NGOs and ICT stakeholders to share their experience of government modernisation.

Managing Director • **James Smith**
james.smith@alphabet-media.com

Editorial Director • **Jianggan Li**
jianggan.li@alphabet-media.com

Assistant Editor • **Rahul Joshi**
rahul.joshi@alphabet-media.com

Journalist • **Thanya Kunakornpaiboonsiri**
thanya.kunakornpaiboonsiri@alphabet-media.com

Contributing Editor • **Ken Sawahara**
k-sawahara@aj.jp.nec.com

Contributing Editor • **Aw Beng Teck**
bengteck_aw@nec.com.sg

Publisher • **Chris White**
chris.white@alphabet-media.com

Designer • **Nandita Gupta**
nandita.gupta@alphabet-media.com

Designer • **Brigitte Suba**
brigitte.suba@alphabet-media.com

FutureGov Asia Pacific magazine is published by

Alphabet Media Pte Ltd
Bestway Building, 12 Prince Edward Road 03-01, Podium A, Singapore 079212 Fax: (+65) 6324 1228

Alphabet Media Australia Pty Ltd
Level 2, Suite 3, 56 Berry Street, North Sydney, NSW 2060, Australia Fax: (+61) 0 2 8078 6609

Licensed by:

FOREWORD

A REAL OPPORTUNITY TO TRANSFORM

Jianggan Li

Editorial Director
FutureGov Asia Pacific

In 2008, FutureGov published a series of high profile interviews, "the rise of local governments", highlighting the development of city governments and the various challenges they needed to tackle. The visions of leaders of Seoul, Delhi, Beijing, Taipei, Kuala Lumpur and Jakarta were very similar: to cope with complex challenges, to meet a myriad of different expectations and to transform the city to be safer, greener, more efficient and more liveable. Security, for all of these decision makers, was an important foundation to achieve this vision.

These perspectives were shared two years before the launch of iPad, when the prospects of data analytics were at their lowest point and not many people had heard of the term 'big data'. Wow, what a different world that was!

The development of 'smart cities' has progressed in leaps and bound since then. The maturing of some of the key enabling technologies, such as mobility, sensor networks and data analytics gives city authorities unprecedented opportunity to stitch previously disparate security systems together to investigate, respond, pre-empt and prevent. And cross-agency collaboration has become more than just command and control – the ability to collect, transmit and process complex data from multiple sources allows agencies to have much better situational awareness and evidence-based decision making.

Nevertheless, we have to clearly understand technologies are enablers and only enablers. Agencies and decision makers need to carefully assess their situations and challenges, develop the right roadmap, and integrate the right solutions based on their needs and resources. People often say that it is not worth securing something worth one dollar with security arrangements that cost 100 dollars. However, the challenge often is to identify the real worth of the systems or infrastructure to be secured and the real costs of securing them. I hope that through some of the articles in this special supplement, we can explore together how to better and more effectively safeguard cities, their key infrastructure and residents.

The articles are broadly divided into two categories: a series of technology showcases give a comprehensive picture of what can done in each of the areas; and case studies from a few key countries in the region, including China, Indonesia and Vietnam, as well as some best practices from other parts of the world.

If you would like to find out more about the experiences shared in this magazine, FutureGov will be happy to link you with the agencies mentioned; and of course, for more information about the technological solutions, I am sure technical experts at NEC will be more than happy to assist.

Enjoy reading!

FOREWORD

SECURING URBAN ENVIRONMENTS: ROLE OF TECHNOLOGY

Since 2008, for the first time in history, more people live in cities than in rural areas; and according to the UN, urban areas in Asia and Africa will double in population between 2000 and 2030. The consequences of this are deep, wide-ranging, and difficult to overestimate.

Cities have become not only bigger, but also more complex. And the challenge with complex environments is that they are hard to secure–things fall apart easily if we do not plan and act in an integrated manner.

A lot of disasters and disturbances we have experienced over the past year had not been anticipated– this is not negligence on part of public safety agencies, but more a vivid reminder of how complex and sometimes unpredictable the world we are living in is.

At the same time, improved communications capabilities also make citizens more demanding. Delays in response now do the government an immediate and possibly embarrassing harm.

Although we can't control everything, we can certainly build up our capacity to better prevent and respond to disturbances.

While cities in this region have different levels of capacity development, technology readiness and implementation maturity, they have very similar underlying issues to contend with, and fortunately, the same access to information and knowledge.

Now the challenge is in translating information into action. That is where our Regional Competency Centre for Public Safety comes into play.

You probably already know that NEC has a proven track record in public safety. Over the last 30 years, we have installed the world's fastest and most accurate biometric identification systems for more than 480 customers in over 30 countries.

We have developed an advanced and comprehensive suite of safety solutions for use in national identification, law enforcement, immigration, emergency and disaster response, protection of critical installations and safeguarding of cyber infrastructure.

NEC focuses on the development of such applications to serve the needs of the global public safety market. In line with our concept of "Safer Cities", we look forward to bringing our best-of-breed cutting-edge security technologies and total solutions to help public and private institutions safeguard lives and property in the real and virtual world.

Tan Boon Chin

Managing Director,
NEC Asia Pacific Regional Competency Centre for Public Safety

We also realise the importance of capacity building. We help governments and public safety agencies build the necessary human capacity and technological knowhow.

And we are not isolated in Asia Pacific. We are closely connected to our counterparts in Greater China, Latin America, Europe and United States, and will have a uniquely powerful platform that allows best practices across the globe to be shared meaningfully.

I hope the articles in this supplement will give you a good idea of the main issues and offerings at hand.

"'Safer Cities' is an important and integral part of NEC's vision for Smart Cities, in which people live, work, and play in safety and comfort, while also coexisting in harmony with the environment. Although it is challenging to safeguard dense urban areas, we are fortunate to have advanced technologies and solutions that enable us to tackle these challenges. NEC is committed to help administrations in the region make the best out of these technologies, always."

Kiyofumi Kusaka CEO, NEC Asia-Pacific

SAFER CITIES: TECHNOLOGY OUTLOOK FOR 2012

V. Sriram, Consultant, Frost & Sullivan, writes about the challenges of securing modern cities, technological trends to look out for in 2012, as well as the opportunities offered by smart technologies.

Modern cities are facing complex security challenges. Rapid urbanisation, floating populations, technology advancements, natural disasters and global terrorism are all posing significant threats to city administrators and public safety agencies.

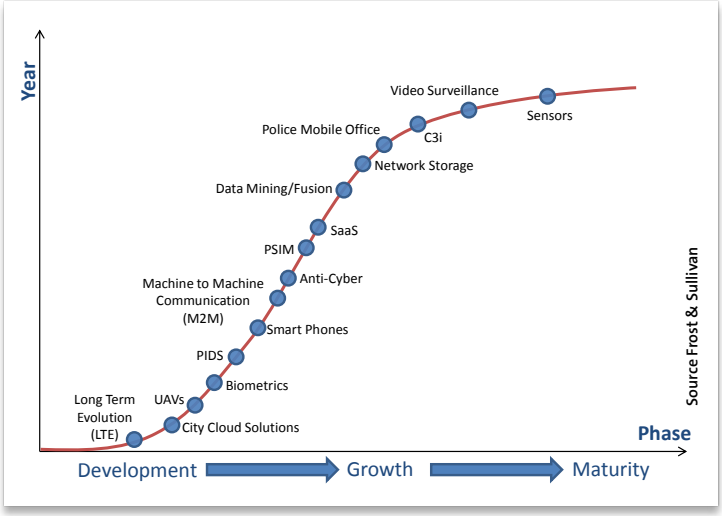
The fortunate thing is while the challenges are becoming more complex, so are the technologies that authorities can leverage to protect cities.

The emergence of smart technologies is driving the revamp of how government handles city administration, including security.

We see that 'Safe Cities' has been made an integral part of 'Smart Cities' master plans that are being planned and implemented across the world.

The modern Safe City concept enhances public security and welfare by deploying networked security systems and capabilities optimally to enhance prevention, detection and response to threats, disasters and other emergencies.

Vast communication and sensor networks across cities enable law enforcement and other public safety agencies to gather greater quantities of data more efficiently. Increasing analytical capabilities of information systems allow authorities to interpret the data meaningfully and respond to events effectively. These technologies also foster greater interoperability and allow



> Maturity levels of key security technologies/solutions

information to be aggregated to give quick situational awareness to authorities, and thus aid decision making.

All these capabilities are driving changes to the way cities evaluate their security requirements.

We also witness the influence of factors such as a strong city economy, availability of IP networks and improved public-private-partnerships in secure city planning and implementation.

TECHNOLOGY LANDSCAPE

Technology is the key enabler of safe cities. With the Safe City concept becoming more popular on a worldwide basis there will be a higher demand for new security solutions. Convergence is happening across industries and markets at great pace and the security sector is no different from other infrastructure related markets such as energy and transportation. Technologies such as video surveillance, biometrics and so on are gradually changing the way intelligence is being gathered and processed.

Indeed, Safe City solutions incorporate a wide array of technologies. With older technology, such as CCTV surveillance, reaching maturity new security solutions are implemented to strengthen the city safety and complement the capabilities of existing systems. The figure above depicts the life cycle of different technologies:

Long term evolution is in its earliest stage of development as far as security applications are concerned. We expect LTE to have a significant impact on security systems in the coming years.

City Cloud Solutions are going to witness an increase in their popularity with the implementation of fast wireless internet connections and a wide array of mobile technologies.

CCTV surveillance, though still in the maturity phase, is an essential part of security and will continue to have a footprint in the security market.

OTHER SIDE OF THE FENCE

The following is a brief description of some of the Safe City projects that have been implemented and are in progress from outside this region.

NEW YORK

City Scenario

Having struggled to make efficient use of key data on paper reports and in databases that were not connected to each other, the New York Police Department (NYPD) implemented Real Time Crime Centre (RTCC), a system that integrated all the databases in-house.

The system comprises three key elements which are: data warehouse, data analysis, and data wall.

RTCC allowed the officers to extract information concerning criminal complaints, arrests, and 911 calls in the New York region.

The system is also integrated with a nationwide network to search and retrieve criminal information. RTCC's ability to

communicate with handheld devices has allowed the law enforcement agencies to apprehend offenders immediately.

Result

The concept was estimated to cost US$11 million. The first year after implementation, approximately three quarters of homicides were solved in the City. The officers welcomed the application as it took them much less time to retrieve and analyse data than previously.

The future of this system is further integration with divisions in the NYPD, setting up alerts to extract potential perpetrators, criminals and persons of interest.

Another effort that will follow is the creation of subject matter experts to further investigate criminal activity (homicide, burglary, etc.) using the system. The plan is to continue to expand the number of applications in the system to make the city an even safer place to live in.

LONDON

City Scenario

London faced immense threats of terrorism after 9.11, which escalated to the bus and subway bombings in 2005 that killed 56 people. In order to cope with the increased threat level, London has proposed a solution to integrate their call handling, radio, telephony and CCTV.

The system would connect over 500 workstations, three communication control centres and a multiple number of small control rooms.

Result

The US$64 million project created integrated systems at the disposal of the emergency services that allow first responders to not only react after incidents but also prevent crimes and tragic events from happening.

MEXICO CITY

City Scenario

The capital of Mexico faces lots of security challenges, from petty crimes in the slums to the turf wars of drug lords. In the first five years of the century, the city had an average of 478 crimes reported every day. The actual figure is thought to be much higher, as victims are often reluctant to report crimes.

In addition, the city also sits on a major earthquake belt, and a major earthquake in 1985 paralysed many government agencies, eliminating their databases.

Between 2009 and 2011, the city underwent a major security overhaul; and a major project under this was the "Bicentennial Safe City". The government made investment to install 8088 surveillance cameras across the city, lay 200 km of fibre network as well as establish and staff four regional command and control centres (C2s) and a central command, control, communications and computer centre (C4i4).

The C4i4, which opened in late 2011, is located in a 34,000 square metre compound. The main building is divided into three areas, used for parking, administration and operations respectively.

Fausto Lugo, Director General of the city's Centre of Attention to Emergencies and Civil Protection, explained that dispatching processes and procedures had been standardised for all officers on the street, who report to different agencies and units.

Result

Mexico City Government invested US$463 million in the "Bicentennial Safe City" project. In 2011, the city witnessed a 12.5 per cent reduction in crime rate.

The police have reduced their average response time to less than five minutes. And for the first time Mexico has comprehensive video material for crime research and forensic video analysis.

Going forward, the government plans to include the city's 100,000 private sector surveillance cameras into the system.

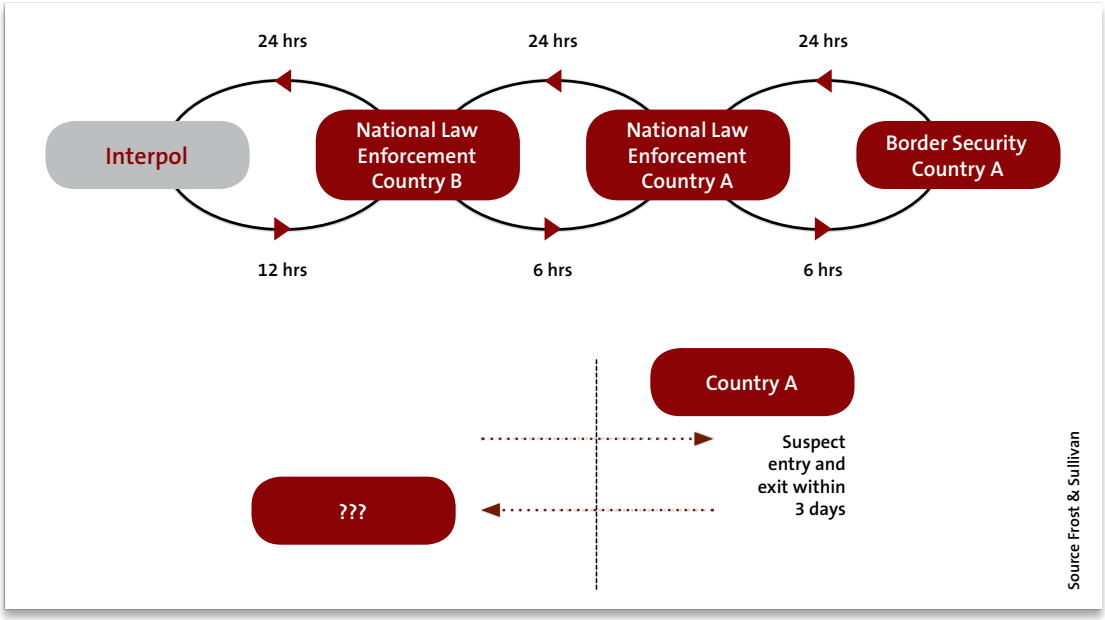
INTER-AGENCY COLLABORATION: THE QUEST FOR INFALLIBILITY

Machine-to-Machine communications and big data tools allow right information to flow between agencies at the right time, with the right intelligence derived. These are the key enablers for public safety and emergency response agencies to collaborate and tackle current security challenges in a timely manner.

Security is becoming increasingly more complex, with the proliferation of sharing of information through the internet, devices and sensors ranging from CCTV surveillance to mobile devices to social media. This has resulted in an exponential growth of data which public safety agencies have to grapple with.

Welcome to the age of big data.

While these data are certainly valuable, to be meaningful they need to flow through relevant channels and be analysed by



> The timeliness of data flow is critical in pre-empting any security breach

the right agencies in a timely manner. For agencies intending to collaborate, they will face the bottleneck of the human capacity to process these data. As the volume of data increases exponentially, the people needed to process it into useful, meaningful data will be limited in number and in capacity.

Fortunately, our capabilities to collect, transmit and analyse data are also growing tremendously. To leverage state-of-the-art technological tools to address the complex issues in this arena, NEC is introducing the concept of an inter-agency collaboration framework (IAC).

ENABLING AND ENHANCING DATA SHARING

IAC enables agencies to manage, filter and analyse the information coming from different sources, and to respond to any threat that is detected arising from an analysis of the information.

The framework will incorporate analytics tools, machine-to-machine (M2M) communications, and the collection and processing of meta-data and sensor data, and the necessary communications systems to fully integrate all sources of information into a seamlessly connected platform that is responsive and agile, and better able to meet mission-critical demands.

In a nutshell, it provides a framework for agencies to collaborate by enabling data to flow and be shared among agencies. It aims to support prevention, assist in detection, signal for response and aid in recovery. Its goal is to be greater than the sum of its individual parts.

TIME OF ESSENCE

As stated, one of the most common challenges which law enforcement and emergency response agencies face today is not only the lack of information being provided to them, but also the time it takes for the information to reach them and, more critically, the time and resources to analyse the data.

Take a simple example of a suspect entering a country whereby border security agency may raise a query with another agency of another country. By the time the information is received by the border security agency, estimated to take four days, the suspect may have already entered and left the country for another destination in a matter of two or three days.

In this case, information has been provided. However, the

time taken for that information to flow to the relevant party, which is of utmost importance, has to be timely. The time taken will naturally depend on the level of security of the case in hand and the height of alertness raised between concerned agencies.

The approach depicted above is a bottom-up approach wherein the query is presented only after a suspect presents itself in the country. An ideal scenario would be a top-down approach where information is already present with the border control personnel through the sharing and ease of flow of information.

With IAC, a large part of the suspect identification and information exchange process would be automated, based on intelligent data filtering and business rules built in according to specially implemented ontology that has been precisely defined to account for such scenarios.

Ideally, the data collection, analysis, and feedback loop should be fully automated. For example, CCTV devices with biometric facial capabilities will identify suspects at ports of entry into a country. This is coupled with other biometric devices collecting information such as fingerprint, iris and/or voice.

Additionally, demographic data is automatically scanned using passport scanners at checkpoints. The information from all these different devices will be automatically sent for matching with the vast repositories belonging, theoretically, to any domain that agrees to share its data records.

The feedback loop from remote border posts to a central repository of data—such as an Intelligent Operations Centre (IOC)—thousands of miles away and in another jurisdiction, could take seconds, with the human factor entirely removed from the equation.

KEY ENABLERS

Because of the explosion in the use of devices, including the advent of mobile devices, the resulting growth in data has been correspondingly explosive. Any agency that attempts to accurately assess a given situation needs to be able to gather all of the relevant data promptly and make timely informed decisions. In order to achieve this, there are primarily two key enablers:

a. Effective Machine-to-Machine (M2M) communication system. As processing power and communication bandwidth among devices far outstrip human-moderated processing power and communication, leveraging M2M communication and the "Network of Things" will prove pivotal in the move towards seamless IAC.

Cloud devices will sit on top of the Cloud platform and the network, which will provide the communications service. While mobile computing and the internet have brought to the surface unimaginable potential in complex, multi-party communication, most of this is limited to human-to-human communication, with M2M interaction largely restricted to on/off control and simple data aggregation.

M2M communication has the potential to evolve as a parallel network to the "human" internet, where "human" and "device" data interact at the platform level. This will revolutionise information exchange by removing the human bottleneck.

b. Analytics and Big Data tools. The Cloud platform needs to interface with Cloud services that will handle the data accumulated by the devices in a meaningful way. A service that is critical in large-scale emergency or other public security operations is real-time data-crunching mechanism leveraging on sophisticated analytics tools to streamline petabytes of data into useful, actionable and human intelligible output.

Analytics tools are reaching a level of sophistication where meaningful conclusions can be derived with huge amounts of input data. This can all be achieved through automation and business rules, which is otherwise humanly impossible.

With all these capabilities, command and control centres are no longer merely performing a command and control operation. They have become the centre of critical information control, the real brain of security operations, making informed and timely decisions to protect and safeguard our cities, properties and lives.<

SAFEGUARDING KEY INFRASTRUCTURE: AN INTEGRATED SECURITY APPROACH

Integrating disparate security systems through biometrics, identity management and mobility allows for faster response, better investigation, efficient processes and comprehensive security management.

Imagine when the authorities and operators of a critical facility receive a phone call with the message "a lady in her forties, with blond hair but believed to be Chinese by ethnicity, drove a black sedan into your facilities with 20kg of TNT". Obviously you have visitor registration data, X-ray images, CCTV footage; but when you conduct the investigation, where should you start such that you can stitch all the information together and get real situational awareness?

Currently, most critical facilities around the world, including oil refineries, seaports and border crossings, have various security systems that take care of different areas. Often, relevant information resides in disparate servers and there is no mechanism to pull together all the relevant data to speed up the response and investigation process.

In many recent incidents across the region, authorities have been slow to respond or to issue announcements. One of the key reasons, in many instances, is that data disparity does not allow authorities to have the timely situational awareness they ideally should have.

Similarly, when an airline receives a hoax call, the current standard operating procedure dictates that the airline cannot take chances. Force landings, evacuations and thorough searches are conducted before the plane can be cleared, causing delays and economic loss. If all the subsystems can get together and give the authorities an answer more quickly, a lot of time and resources can be saved.

COMPONENTS & INTEGRATION

That is why an Integrated Security System (ISS) is needed. ISS not only puts together all this information easily, it also allows for mobility, real-time connectivity between agencies, as well as achieving security and cost savings without sacrificing convenience for users.

ISS targets at collecting the relevant information at the right time and using these data meaningfully whenever there is a need.

To achieve that, an effective metadata search engine needs to be built into the system. All the relevant information is associated with a particular ID such that management, response and investigation will all become more proactive.

NEC traditionally places a lot of emphasis on identity management. It has not only the best fingerprint recognition system in the world, but also a proven track record in deploying other biometric solutions including iris scans and facial recognition, as well as identification documents such as passports, ID cards and entry permits.

Combining biometrics with automated data workflow enables the tracing of all the information pertaining to particular individuals. For this NEC has identified top

six security areas to focus on: intrusion detection, IP video surveillance, access control, visitor management, human tracking and public address/fire alarm.

A UNIQUE BIOMETRIC IDENTIFIER

In each of these areas careful planning and calibration is needed. For example, the road blocks need to be designed so that a car blowing up will block only that lane but not other lanes; fence sensing systems need to be combined with high-definition CCTV for intrusion prevention; and better algorithms need to be developed to ensure optimal analysis. Putting all of these together, the automated standard operating procedure (SOP) should be not only trusted, but also embraced by end-users.

Although RFID and biometrics are becoming common, in many installations around the world, pedestrians and vehicles entering the facility are verified in different ways. It is usually an easier process if the passengers are on wheels, because the authorities and facility operators do not want to hold up the traffic. However, clearing individuals at the turnstile and at vehicle checkpoints should be the same. For instance, pedestrians will need to tap their RFID card, have their faces or fingerprints scanned, pass through a metal detector and have their luggage X-rayed, before they are completely cleared. Fingerprints will be used as the sole identifiers for all the data and images associated with this individual. It makes the person entirely responsible for what he carries.

> Critical infrastructure, the bloodline of modern metropolises, is especially vulnerable to security threats

NEC is advocating the same SOP for vehicle clearance. Whether an individual drives a motorcycle, a private car or a delivery truck, his or her fingerprint will be captured, and used as the identifier for all the information associated with this vehicle captured into the system by different applications. This can be under vehicle screening, x-ray, licence plate recognition and CCTV surveillance. In addition, fingerprints of all the passengers will be captured as well and stored in the database. All these data will form one entry at the backend, with the driver's fingerprint acting as the master identifier.

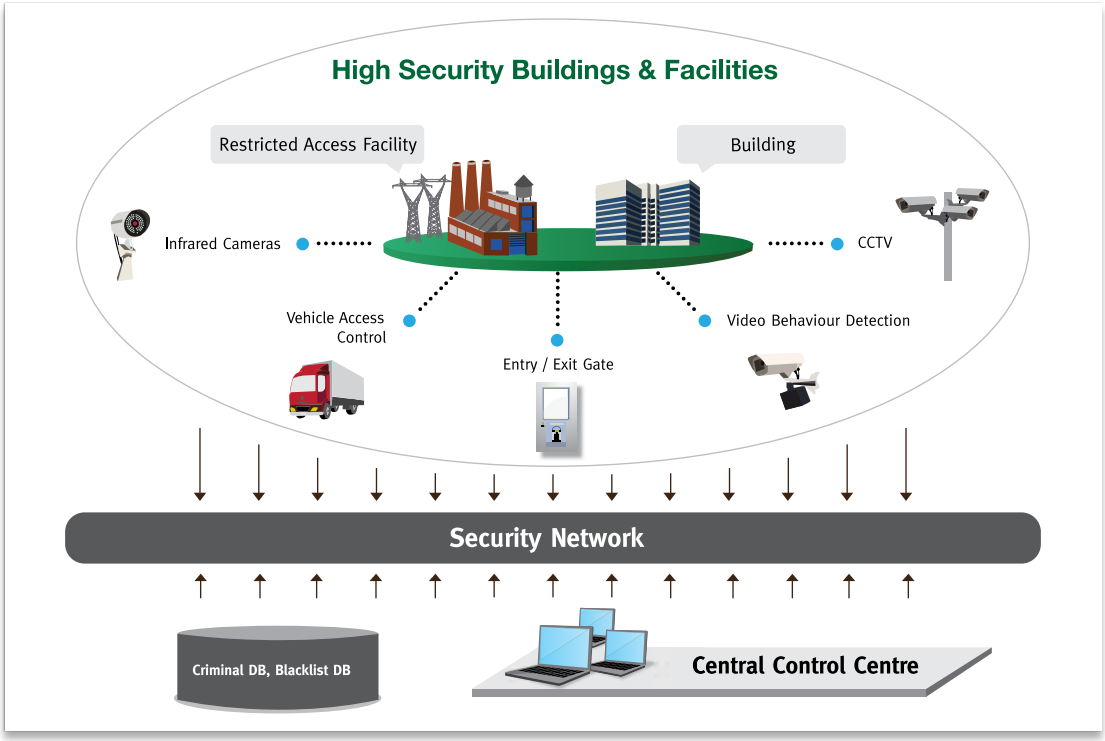
In this way, accountability is ensured upfront by tying all the previously disparate strands of information together. When a metadata search is conducted later, it becomes unnecessary to stitch information together from different servers. And it enables accurate, comprehensive information to be retrieved much faster.

An additional benefit of introducing biometrics is that the same access control system can be deployed throughout your facilities globally, thereby creating an integrated and highly-secure environment for your organisation.

FACIAL SCREENING

Also incorporated within the ISS concept is facial screening. Facial screening uses the same concept as metadata search with a set of parameters; it captures different images of an individual and stores them in a database for possible verification and comparison.

One such system is now deployed at Hong Kong International Airport, where high-speed cameras capture eight images of each arriving passenger as he or she passes through the aerobridge to reach the terminal. The images are then used to match against a watchlist at the backend, and the system alerts the authorities in case of any suspicious individual arriving.



> The basic elements of an Integrated Security System

IMPLEMENTATION CONSIDERATIONS

ISS is currently deployed at a major facility in Southeast Asia, which is expected to become the first in the world to have all the security elements integrated, allowing better proactive response, fast investigation, and ultimately, better security.

SOPs are a very important factor contributing to successful ISS deployment. They should be developed with rigour and reviewed thoroughly after implementation.

User involvement at the early stages is critical. The highest level end-users, who are on the ground and who will be directly involved in the day-to-day operations, could be the champions and the spokespersons right from the blueprint stage. Their early involvement allows optimisation of the SOP, as well as managing changes when the system is rolled out.

A project will not be ISS-ready unless the command centre is integrated. All the intelligence can be collected and integrated, but ultimately, a command structure that ensures all the information is put to right use at the right time must be established.

In most cases, the ISS needs to be operationally available on a 24/7 basis. Ensuring round-the-clock availability requires a careful look at the architectural design at the very early stages, building in backup to make sure all the data are available and can be pulled out in any circumstance.

IDENTITY LIFECYCLE MANAGEMENT

While the above framework allows different biometric input stations to be linked at the backend, the importance of Identity Lifecycle Management (ILM) must be emphasised. An individual's access to the facility may change over time, depending on their role and seniority. They might also leave the system and enroll again at a later stage. What is needed to be built into the system is the ability to recognise these individuals such that they do not have to go through complicated processes.<

THE LAST LINE OF DEFENCE FOR ONLINE SECURITY

A key aspect of safeguarding information flow from and to city servers is the security framework that forms the last line of defence in the protection of critical data. Wong Onn Chee, Director of iNFOTECT Security, talks about pioneering intelligence solutions for servers that take cyber security for cities to the next level.

Making an entire city impervious to cyber-attacks is a daunting task. The technological and regulatory infrastructures in place play a central role in ensuring that data remain where they should and are only accessible to legitimate parties. The monumental effort in coordinating the safety and validity of data stored in servers, in mobile devices, and all other containers of digital information requires techniques more sophisticated than mere brute force.

What are the security risks associated with cloud computing? How can they be mitigated?

Security risks from cloud computing are no different from the risks one faces when outsourcing the hosting of data and applications to a provider. My personal view is that cloud service providers should be regulated and licensed, just like banks and telcos. When we talk about utility computing, we tend to forget that the traditional utilities providers, such as water and power firms, are all regulated and licensed.

And if information is the currency of the New Age, clouds contain lots of information, and thus should be treated like regular banks—and regulated. The current practice of having each cloud service user evaluate the security profile of every cloud service provider is not efficient.

Today, when we go to a Singapore bank to deposit our funds, we do not ask the bank teller for the bank's security policies, disaster recovery plans, access control policies and other security information. This is because banks in Singapore are regulated by a central and impartial authority—the Monetary Authority of Singapore (MAS)—and people trust the MAS to properly monitor and assess the security risks of banks in Singapore.

That's why having a regulatory and licensing regime to govern cloud service providers will increase confidence among cloud service users and spur higher cloud adoption. As we all know, one of the main obstacles to cloud adoption is the risk of data leakage. With proper regulatory oversight, the leakage risks of cloud can be mitigated by mandating that all cloud service providers put in controls to prevent information leakage. The current "Wild Wild West" situation among cloud service providers is not conducive to increasing consumer confidence in cloud computing.

How does mobile computing factor into the equation, with its widely distributed end-user devices and the accompanying complexity of information flow?

The increased computing power and storage capacity of today's mobile devices present a new paradigm to security professionals. With more enterprise data being accessed from mobile devices and stored on them, the leakage risks are higher. Data are often stored on mobile devices without encryption and when the mobile devices are lost, sensitive corporate information is also lost. In addition, mobile malware is increasing in volume and it will be the next frontier for security professionals to tackle. Mobile computing will make leakage protection more challenging.

Wong Onn Chee

Director, iNFOTECT Security

Can you walk us through a few typical and atypical scenarios of leakage, and the best practices to prevent them?

There are several means of information leakage. Common ones include leakage from removable storage media, email and external web 2.0 portals. The less common but equally damaging ones are leakage via peer-to-peer software, stenography (hiding information in images, audio and video files), physical paper documents, and even verbal conversations.

Existing solutions do not detect or prevent information leakages from our corporate portals. One can refer to the reported incident during the Singapore General Elections 2011, in which personal information of candidates was inadvertently displayed on the Singapore Election Department's web site before being taken down. The identification number, mobile phone number and address of the Prime Minister were all leaked in a PDF file.

Singapore has a Cyber Watch Centre (CWC) that monitors all the government web sites round the clock. Unfortunately, the eyes from CWC are all trained in monitoring incoming requests; when sensitive information like this leaks out, nobody notices. In the end, newspapers, not CWC, reported this leak.

There are numerous such examples of country-wide and city-wide attacks. In Japan, a virus affected administrative PCs–and because it was a zero day variant, of course no anti-virus caught it. They attacked the web service, and 73,000 visitors got their usernames and passwords stolen. The virus then modified ASP and HTML pages and the visitors got tricked into installing malware on their computers.

Then there's the case of UBS, Singapore in 2009. A careless technical error during upgrade results in the leakage of information of all private banking customers in Singapore and Hong Kong. UBS was regulated by MAS and they have in-bound protection system, but once information leaks out, all it can say to MAS is: "I did not violate your security policy – I complied with everything."

Princeton Review (PR) is a reputed organisation that deals with higher education statistics and data. A competitor doing market survey on the PR web site, to its pleasant surprise, found 108,000 confidential student records freely available to access. Washington Post was alerted, which subsequently published a news story about this leak.

That's why innovative solutions are required to address the leakage risks from corporate portals. The impact of information leakage from corporate portals is a thousand times more severe and damaging than losing a USB drive.

For instance, when sensitive information is leaked from your corporate portal in Singapore, anyone on the other side of the world can view the leaked sensitive information a second later with a click of a mouse. However, one cannot say the same about the speed and extent of leakage when a USB drive is lost. Similarly, when your corporate portal is leaking information, the whole world can see it and will know. But when your USB drive is lost, it is unlikely the whole world will know.<

Besides being Director of iNFOTECT Security, Wong Onn Chee is also the current Singapore Chapter Lead for Open Web Application Security Project (OWASP) and a member of Security & Privacy Technical Committee under Information Technology Standards Committee in Singapore. iNFOTECT's flagship product iNSIGHT for Web Server (IWS) is a dedicated outbound security solution for web and cloud services. NEC Asia Pacific is the exclusive marketing and channel development partner for IWS in Asia Pacific.

COUNTERING COMPLEX THREATS IN SPRAWLING INDONESIA

In 2009, Indonesia's Immigration Authority introduced biometric passports in order to manage border access to a nation of 238 million people across 17,508 islands. Erwin Azis, Director of Immigration Information Systems at the Directorate General of Immigration, Indonesia, reveals the pioneering journey that his department undertook— and the subsequent triumphs and challenges— in a conversation with Rahul Joshi.

While the militaries of modern nations continue to defend them against large-scale armed conflicts, the advent of terrorism and its accompanying tactics of guerrilla attacks and distributed, covert planning has placed the effectiveness of civilian security forces in an equally bright spotlight.

For a country like Indonesia, this role is made doubly complex because of its widely diverse demographics and geography, along with a massive population and a gradually—but steadily—developing economy.

Indonesia's Directorate General of Immigration (DGI) passport offices, for example, are distributed across 108 locations within the country, making the construction of a centralised database storage and access system a daunting task.

The Bali bombings of 2002 proved to be a wake-up call, however, and the only possible positive outcome from the tragedy was that it catalysed a complete transformation of the country's national security infrastructure.

The Indonesian biometric passports, available to citizens at just IDR 405,000 (US$48), work on a distributed-node/ centrally-processed biometric-matching system. Legacy data took just two months to migrate to the new system, in which existing facial and fingerprint records were stored in a new format.

Data are captured at any of the sanctioned offices across the country and consolidated in a centralised database system in Jakarta, belonging to the Immigration Headquarters.

The server farm in Jakarta is capable of matching 400,000 fingerprint and facial records per second, which is used to verify and manage citizen records and identify and eliminate duplicates.

The introduction of biometric passports has proved to be not only successful but also a country-wide learning

Erwin Azis

Director of Immigration Information Systems at the Directorate General of Immigration, Indonesia

experience in ICT, project management, data management and security responsiveness.

As the Government gets ready to phase out its old passports by 2015, Azis takes us through his background—he started his career in law, not in ICT, which ironically proved to be advantageous in certain aspects of project implementation—and the skills and organisational nous required in implementing

> Indonesia has the world's 4th largest population and a dozen cities with more than a million inhabitants

the biometric passport system, along with the demands, trials and achievements along the way.

What are the main issues that you have to deal with in terms of security? What was involved in the preparation phase of the system?

Although I came from a law, rather than IT, background, I understand the logic of IT, which often proves to be very useful in project planning and execution.

I have a great team to support me, so that when I say I want something specific, it is able to interpret what I mean.

Over the past three years, I have acted as the director of IT, and my job is to improve our IT development. Security concerns are of primary importance, that's why we learn from Singapore, from Malaysia, from Thailand, and also from Europe.

In the meantime, we have been preparing our human resources; we're preparing our team of about 30 IT specialists. We have also been building the capacity for local immigration officers across Indonesia.

The funding was contributed in part by the Ministry of Finance, with the rest coming from our own budget. 70 per cent of the money that people pay to make passports goes into funding the project—this has proved enough for our purposes.

We have a data centre at the head office, but every immigration office also stores and processes its local data. We have another centre in Bali dedicated to backup.

Since the Bali bombings in 2002, has there been any change in the way you operate?

We now try to be faster. The lessons we have learnt from the Bali bombing is very important for our side—we have to control who enters the country, and who goes out of our country. In the older system, data movement rate had reached an upper limit, which this system corrects.

That's why right now, if an Indonesian citizen possesses more than one passport, he or she will not be able to apply for another passport with a different identity. We identify duplicates from fingerprints and facial scans.

Our system will also detect if someone is being watched by the police or by another agency. For example, if the police are trying to catch a suspected terrorist, they will be alowed to access our data centre and search for relevant information about the suspect.

Do you cooperate internally with other agencies, and with your peers internationally?

Recently, we have received a lot of visitors from different countries. They include delegations from a number of agencies in Malaysia: last January, an agency from Sarawak approached our centre. We receive one delegation from Australia almost every three months; our counterparts in Singapore have already visited us about five times. We have also visits from the US embassy and even from Israel.

We have been cooperating with the Indonesian International Organization for Migration, while the budgeting support is from Australia, which covers our costs of training. Almost all the training that we needed, such as in security, in database building, in programming, came from Australia, and partly also from New Zealand.

We are cooperating with the

> Data for e-KTP are captured at any of the sanctioned offices across the country

Kementerian Dalam Negeri (Ministry of the Interior) on the Kartu Tanda Penduduk (KTP), which are identification cards for citizens. We are sharing our experiences on how to build the system, and especially on how to prepare the manpower required. The KTP project is well on course and is expected to be completed in about 2 years.

We will incorporate the KTP number into our passports in the future. The information stored on the electronic KTP cards also includes iris scan images, in addition to fingerprint scans and photographs.

Many agencies in Indonesia are now learning from us how to build, how to prepare, how to fund, and how to cooperate with other agencies in building large systems.

Almost every week, members of the police and officers from anti-corruption and anti-narcotics agencies come to our office to learn from our side. Many agencies here had tried to build a similar system in the past, but failed in the process.

What was the main problem they encountered?

The most important thing is the human resource. The agencies have to change the culture and change the mindset of all the stakeholders involved —instead of just focusing on securing the funding. They also need to understand that they have to plan and prepare this system from scratch, and not just build on top of an existing system.

What are your plans for the future? Will you also be using CCTV at border control?

This year, we are working with Soekarno–Hatta International Airport in Jakarta on implementing a CCTV system. Auto-gates for electronic passports that provide automated check-ins are already implemented there, and all of these systems are fully under the purview of the DGI.

We will review our existing IT system next year as it is already five years old now. We will look into new hardware and new software—technology changes day by day, and we are looking at refreshing our system by the year of 2013.

Right now, the biometric identification system is implemented at 45 locations and ports across the country.

In the near future—assuming adequate funds are available—we will look to build more stations which will use the system.

I will be leaving for Europe shortly to learn more about the electronic passport systems in France, the Netherlands and Switzerland; I want to learn about laminating, and how they build their systems from the ground up.

My view has always been that the more knowledge you have, the more it opens up your mind.<

KEEPING PACE WITH ONLINE AND IDENTITY THREATS IN VIETNAM

A number of initiatives have been launched by Vietnam's Ministry of Public Security. Major General Dr Nguyễn Viết Thế, Director General of the Ministry's IT Department, shares the details of these projects with Jianggan Li and Ha Doan.

Vietnam has undergone significant economic and social transformation in recent years. Rapid urbanisation and city development have brought tremendous security challenges for the government, as the agencies struggle to modernise their workforce, infrastructure and services to cope with emerging threats, both physical and virtual.

Major General Dr Nguyễn Viết Thế, Director General, IT Department, Ministry of Public Security (MOPS) says that one of the biggest security threats comes from the cyberspace.

"Although government agencies at the central, provincial and local levels are moving more and more information and processes online, protection of their IT infrastructure has not kept up," he notes.

During the first half of 2011, hackers managed to penetrate many government web sites and systems, generating a lot of public concern about the security of government IT infrastructure.

A MOPS study last year showed that more than 60 million computers in the country were infected with virus or malware, or both. The Ministry also detected an increase of counterfeit anti-virus software last year, which opens security loopholes rather than protects IT systems.

Dr Thế believes there are many factors contributing to this alarming landscape, including lack of human resources, lack of protection tools, lack of web management expertise and lack of security awareness.

Often, government organisations plan and implement IT projects without sufficient protection built in, and fail to take prompt actions when alerted for security breaches.

He explains that the solution for all these challenges boils down to two things: funding and training; the government is serious in addressing this problem.

In 2010, the Prime Minister issued a 10-year plan to bolster the country's defences against cyber attacks and cybercrime; and MOPS has been tasked to implement the plan.

The Ministry will allocate resources to train cyber security specialists as well as government end users of IT infrastructure and services.

The plan also includes investments to install firewall, intrusion detection and prevention systems (IDPS), encoding technologies and secure authentication on web sites and IT systems.

In addition, the Ministry has set up a Department of Cybercrime policing, which works closely with Vietnam Computer Emergency Response Team (VNCERT) in cyber policing and emergency response.

Legislations are being prepared at the parliament to explicitly criminalise cyber attacks.

MOPS, which is essentially Vietnam's Ministry of Interior, also handles many areas of public safety, including policing, fire fighting and immigration. To improve safety of cities, surveillance cameras are being

installed to monitor traffic, crime and other incidents.

A major surveillance project that MOPS has undertaken was the instalment of cameras along the 35 kilometre Pháp Vân - Cầu Giẽ highway in the capital city of Hanoi, which was funded through official development assistance from the French Government.

The system is now operational, and the MOPS is trying to secure more funding from itself or the Government of Hanoi City to install more cameras.

IDENTIFICATION FOR CITIZENS

The Ministry is also working on the ID card production and issuance project. The provision of a modern ID is expected not only to lower social transaction costs, but also to help government manage security operations especially in urban areas.

The project was originally planned to be implemented between 2008 and 2014; however because of the delay in funding, the start was delayed to 2010. The state has budgeted ₫600 billion (US$30 million) for the project.

Dr Thế explains that the delay was due to the funding and procurement cycle for all IT-related projects in Vietnam.

For the above-mentioned projects, MOPS submitted the proposal jointly with the Ministry of Finance and Government Office. The proposal will then be included in the master plan that the Ministry of Information and Communications submits to the Prime Minister. The funding will be released by the Ministry of Finance once the Prime Minister approves the project.

A related project is Citizen Database Management, which received ₫1 billion (US$48,000) funding from the General Department of Police.

The project aims to give the government a comprehensive database of all residents, allowing better security planning and swift police investigations of incidents.

The commencement of the project was subsequently postponed to 2009, when additional funding of ₫7 billion (US$336,000) was released for a consultancy contract to plan and execute the project. The Department has chosen the e-Government Centre of the Ministry of Information and Communications as the consulting partner.

The biggest focus for the Department in 2012, according to Dr Thế, is the e-passport project.

The ₫1 trillion (US$48 million) funding for the project is used for four sub-projects, including the ₫175 billion (US$8.4 million) sub-project to procure equipment and software for e-passport production, and the ₫512 billion (US$24.5 million) sub-project to install the technical infrastructure, equipment and software for issuance.

Proper control and management will also be developed in agencies under the Ministry which will be handling the production and issuance of e-passports.

Dr Nguyễn Viết Thế

Director General of the Ministry's IT Department, Vietnam

Authentication technologies including biometrics and RFID are also being used for the project.

The project, which was approved by the Prime Minister in 2010, is expected to take four years to complete.

In the first stage (2011-2012), MOPS expects to start producing and distributing e-passports across different local bureaux across the country.

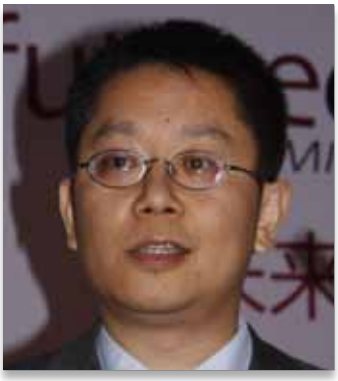
In the second stage, between 2013 and 2014, similar capabilities will be implemented at Vietnamese embassies and consulates across the world; in addition, e-passport control channels with fingerprint readers will be built at the major border ports in the country.

Currently, the Ministry is choosing the consultancy partner for the project. Thế says e-passports and the other major projects will keep him 'very busy' in 2012.

TEAM UP TO KEEP BEIJING SAFE AND HARMONIOUS

Song Gang, Director of Information Systems and Equipment Service Centre, Beijing Municipal Bureau of City Administration and Law Enforcement, shares with Jianggan Li the concept, processes, technology and inter-agency collaboration in city management.

January 22 this year was the Lunar New Year, where hundreds of millions of Chinese travel home for reunion dinners. However, for Song Gang, Director of Information Systems and Equipment Service Centre, Beijing Municipal Bureau of City Administration and Law Enforcement (BCALF), it was the 10th Lunar New Year he had to spend at the Command and Control Centre.



Song Gang

Director of Information Systems and Equipment Service Centre, Beijing Municipal Bureau of City Administration and Law Enforcement

Beijing allows its residents to set off firecrackers and fireworks in urban areas during the Lunar New Year period, and the bureau is in charge of monitoring the firework situation, enforcing the ban on illegal firecrackers and managing the environmental impact.

In fact, BCALF 's law enforcement responsibilities cover a huge spectrum: environment management, river management, pollution control, sanitation, street vendor management, outdoor advertisement, car park management, municipal dispute resolution and 'low-level crimes'.

The bureau, which employs 6000 officers, also works closely with other authorities to maintain the safety and harmony across the 14 districts and 2 counties of the City. A law enforcement brigade and a Command Centre are operational in each district.

GRID MANAGEMENT

BCALF is a heavy user of geospatial information systems. In addition to equipping officers with trunk radio, GPS and mobile data terminals, the Bureau also prides its service for its "grid management" paradigm that enables clear responsibility and close collaboration of different bureaux on the ground.

Using a digital map platform, the city is divided into small geographical units, called 'cells', which became the basic units for management. Resources will be allocated to these cells according to their size, population and complexity.

The concept was first implemented in Dongcheng District, a developed urban area. Its 25.38 square kilometres District was divided into 1652 grid units. Each unit was monitored by assigned city administration inspectors. The monitoring and operational functions were separate, ensuring that inspectors could monitor the execution while the operations departments could focus on their job. The clear accountability and division of responsibility helped improve

> City Administration & Law Enforcement Command & Control Centre in Haidian District, Beijing

the efficiency of response to security and other issues in the city.

All the public facilities, including lampposts and manhole covers, are coded and mapped into the system. In addition, inspectors are equipped with mobile devices for efficient data entry and transmission on the ground.

Song says the system has forced bureaux and departments to work together and devise a lot of processes for joint operations.

Similar grid-based city management was also implemented in other districts of Beijing, with modifications based on local context. For example, the northwest Haidian District has a large area and also has a big floating population. Deploying human resources on the ground to cover the entire District would be very costly, thus video surveillance was implemented to complement the city administration inspectors.

The District also consolidated the City Administration Command and Control Centre with the Government Call Centre, in order to not only respond more efficiently to incidents, but also achieve savings through process streamlining.

COLLABORATION & STANDARDISATION

The municipal government and each department have made contingency plans for collaborative response under various scenarios. Song takes the example of heavy snowfall to illustrate how their contingency plans work. The meteorological bureau will inform all the relevant bureaux and departments about the incoming snowfall. The Traffic Management Bureau will dispatch additional officers to the streets.

The Bureau of City Management will engage contractors to clear the snow on streets – a rather complex operation considering the size of Beijing. "We have to do that before the actual snow, otherwise our contractors' vehicles and personnel might be blocked by snow, and not able to reach their workplace on time," Song explains.

As the major problem associated with snowfall is traffic, the command centre of the Traffic Management Bureau will act as a frontline hub to collect information, monitor the situation and coordinate the response. Video streams are shared among the command and control centres to allow each bureau and department to allocate their resources. The city government Command Centre will also be actively monitoring the situation.

Song highlights that while the importance of standards in interagency communications

> Agencies work together to ensure the city of 20 million residents is safe and prosperous

and collaboration is well understood, authorities need to be clear that the making of standards is a progressive process.

The challenge, often, is that when the government went in to standardise, they were facing not a piece of blank paper, but a disparate set of systems already deployed by various departments.

The basic approach of the municipal government was to decide which department owns a 'de facto' standard. For instance, if one bureau owns 80 per cent of the operations of a particular system, then the standard to be developed will be largely based on what this bureau has already implemented.

"In fact, information exchange standards are easier to make and implement than communications standards," says Song. "We have the expertise of interfacing data systems, however standardising the communications would require significant commitment form agencies which had already made investments in infrastructure."

The communications across different agencies on the field are standardised through an 800MHz trunk radio system.

As for Song's Bureau, he explains that as the department is relatively new, there are less problems of legacy. Nevertheless, he stresses that the Bureau must have adequate technological expertise and service capacity such that the standards and systems will be easily pushed to districts and counties. "If they are better in this capacity, they will be truly willing to adopt standards we make and systems we develop."

FUTURE

A new five year master plan has been made for technological development and revamp across the department. A key area is the upgrade of the current Windows-based mobile data devices that law enforcement units are using. Song is conducting a study on the feasibility of using the Android platform for the upcoming generation.

"The reason being that Android is an open system, which makes it easier for us to develop applications and upgrade the system whenever necessary," Song explains.

As the data terminals rely on operator network, Song expects to engage telcos for the procurement of devices and data services, while applications will be developed by the bureau.

This year, a new Command and Control Centre, which covers two stories of floor space, will be operational, with a bigger display system that gives better situational awareness, including the location of all the law enforcement vehicles operated by the bureau.

Song also expects the wide adoption of sensor networks will open up lots of new possibilities to manage and secure the 20 million people metropolis.<

OPENING THE DATA FLOODGATES

Flooding has plagued major parts of the Asia-Pacific region since the monsoon rains in 2010. Rahul Joshi and Thanya Kunakornpaiboonsiri investigate how Japan and Thailand have coped with floods using ICT solutions, and how an integrated management system that monitors all environmental aspects concerning water bodies is a step in the right direction.

The advent of mass media and electrical systems marked the first steps in automated flood monitoring during the early 20th Century. The information age has revolutionised data processing and collection - meteorological tools and water-level sensors are now able to predict possibilities of flooding to a very high degree of precision, and in real-time. Social media has transformed the mechanics of disaster information management—the Minami Soma City mayor's SOS appeal on YouTube during the Fukushima nuclear incident remains an iconic image.

The challenge, however, remains the sheer scale of flood areas and the diverse geographical and demographic landscape they encompass. An integrated, end-to-end flood monitoring and response system can ensure that all the parameters that could have a significant impact on peoples' lives, such as rainfall, water levels, flood spread, census figures and telecommunication disruptions are readily available as data, and updated in real-time if they are subject to rapid changes. The intelligence gathered from this monitoring can be processed and analysed into actionable steps.

2011 marked a dark year for several countries in the Asia Pacific region: Thailand lost 1,425 billion Baht (US$ 45.7 billion) and 815 lives to flooding, while floods in Queensland, Australia created a hole the size of A$30 billion (US$ 28 billion) in the nation's economy. In December, the Philippine President Aquino declared a national emergency, where floods forced over 60,000 people out of their homes as the tropical storm Washi lashed the country's coasts, ultimately killing over 1,200 people.

Dr Sak Segkhoonthod

President and CEO, Thai Electronic Government Agency (EGA)

INFORMATION COLLECTION IN THAILAND FLOODS

Dr Sak Segkhoonthod is the President and CEO of the Thai Electronic Government Agency (EGA), which has played an active role in countering the effects of the floods, as the Disaster Alarm Centre and the Thai Meteorological Department fall under the MICT.

"The EGA's duty was to bridge the government bodies relevant to the situation, and integrate all the elements of information related to flooding. In the future, all information related to natural disasters shall be put into our cloud system," he says.

During the floods, the EGA also integrated pertinent information from several different sources to help citizens in their daily lives. "We pinpointed the location of functional ATMs and open petrol stations, and mapped all these facilities onto a single map, so

> ICT played an important role mitigating floods in Bangkok

people could easily find useful services nearby."

Segkhoonthod considers ICT the most important factor in a disaster situation because "all decision-making is made based on information." The EGA is seeking to integrate all information under the same standards and to make sure citizens understand this information. "For example, if it's said that their house is at a certain sea level, people should know what it means and how it impacts their situation. This is what we missed during last year's floods."

The EGA is also looking into developing more efficient search engine tools to provide up-to-date information to people. "Google, as a search engine, was of little use during the flood, as the information on it was not up-to-date enough, compared to the social networking web sites."

Segkhoonthod also suggests that the private sector and the citizenry were more efficient in sharing information than the government. "Many divisions and government bodies communicated to citizens during the floods using social media, but differing information from different government sources confused people, instead of being useful to them." The information from government, he explains, should be broadcast out of a single department specially assigned that task, to ensure that it is reliable and trusted.

MANAGING RIVERS TO MITIGATE FLOODING

Japan's experience in managing floods has a history that is at least a hundred years old. Its first river management laws came into effect in 1896 and were last revised in 1997. The new laws regulate the "establishment of integrated river management systems for flood management, water utilisation and environmental conservation." The consequence was that the local environment had to be carefully conserved, with governmental supervision placed at the core of river management efforts.

Susumu Tanaka, Chief Manager, Social Systems Operations Unit, NEC Corporation, affirms the need for governmental support in explaining the processes involved in NEC's River Information System (RIS), an integrated platform that monitors flood information.

"Observation data are collected in the control room of the branch office and delivered to the Ministry of Land, Infrastructure, Transport and Tourism or the Meteorological observatory, where it is aggregated and processed."

"Statistical data can be used by officials and shared with municipal offices as well as residents through the internet," Tanaka says, emphasising the critical aspect of mass outreach.

The data collection by observation stations, statistical processing by control rooms, data exchange with relevant organisations, and providing information to municipal offices and residents are all integrated under a single system, which provides a seamless pathway through flood response. "All the systems are made by NEC, enabling prompt troubleshooting and maintenance support," opines Tanaka.

"Even if lines are disconnected due to a disaster, statistical data operations are possible at the branch office with the system's decentralised configuration," remarks Tanaka.

Meanwhile, information related to sediment disasters is provided to residents through a Sediment Disaster Warning Information System, in which downstream pictures of a river are recorded with a surveillance camera. Finally, rainfall and water level data can be linked to the camera pictures, and images taken before and after disaster can be compared for a comprehensive overview of the damage.<

We Make Cities Safer

Improving public safety provides peace of mind and enhances quality of life. Through proven IT and network expertise, NEC provides innovative integrated solutions that safeguard borders, bolster law enforcement, quicken disaster relief and much more. The Regional Competency Centre for Public Safety founded by NEC in Singapore empowers public institutions to implement optimized solutions that protect people and property. With a little help from NEC, both the physical and virtual worlds are becoming safer.

Learn how you can partner with NEC **www.nec.com/security/**

For further information, please contact
NEC Asia Pacific Regional Competency Centre for Public Safety
public_safety@nec.com.sg

Empowered by Innovation NEC

Solutions to Safeguard Lives and Property

Citizen Services & Immigration Control

Law Enforcement

Public Administration Services

Critical Infrastructure Management

Information Management

Emergency & Disaster Management

Inter-agency Collaboration

Learn how you can partner with NEC **www.nec.com/security/**

For further information, please contact
NEC Asia Pacific Regional Competency Centre for Public Safety
public_safety@nec.com.sg

Empowered by Innovation NEC