NEC PUBLIC SAFETY WHITEPAPER

Orchestrating a brighter world NEC

A CITY PLANNER'S HANDBOOK TO PUBLIC SAFETY

Seven key security areas for every city

WE MAKE CITIES SAFER

Using technologies to safeguard lives and property

TABLE OF CONTENTS

EXECUTIVE SUMMARY

As cities grow and flourish, they also face increasingly complex challenges, ranging from the immediate needs of their citizens to long term security.

To deal with immediate safety concerns, city planners need to have robust emergency preparedness schemes and the capability to manage both physical and virtual crimes. But cities also need to take the long term view and plan for renewable energy, green buildings and waste reduction.

Technology can play a significant role in helping cities respond to security challenges. This handbook outlines seven major security areas where cities can use technology to their advantage:

- Biometric identification systems, which have the potential to reduce human error and processing time at borders, will enhance **citizen services and immigration control**.
- Facial recognition systems and other predictive technologies will shift **law enforcement** from reactive to proactive.
- Automated surveillance systems will reduce the dependence on human labor and provide round-the-clock monitoring of **critical infrastructure** such as power, water and telecommunications services.
- Electronic security measures will protect sensitive **public administration services** from virtual risks, while data analytical tools can predict disease outbreaks.
- Strong **information management**, through enhanced security measures and data protection schemes, will help institutions and corporations defend against cyber-attacks.
- On-demand systems that integrate information, analyze the data and communicate with first responders and the public will help governments respond to **emergencies and disasters** quickly.
- Technology platforms will facilitate efficient collaboration between different branches of the government, enhancing **inter-agency collaboration.**

INTRODUCTION

Cities concentrate both human and capital resources, thereby promoting social and economic progress. In East Asia, the urban population produces 92 percent of the region's wealth. Generally speaking, urban populations tend to be better off than their rural counterparts, with greater access to public services such as transport, education and healthcare, as well as higher literacy rates and life expectancy.

Driven by these benefits, the global population has tended towards ever increasing levels of urbanization. As recently as 1990, less than 40 percent of the global population lived in cities, according to World Health Organization (WHO) estimates. Presently, more than half the world's population lives in urban areas, and by 2050, this number will grow to 70 percent. Most of the growth in urbanization will come from developing countries, which are expected to double their urban population from 2.5 billion in 2009 to almost 5.2 billion in 2050.

Statistics such as these are necessary to give a sense of the scale of the challenges confronting governments and city planners. However, it is important to look beyond the statistics to address the people-centric question of what life will be like in these cities. In other words, the focus should not just be on how these future cities can be made possible, but how they will support the people living in them.

Each city may come up with a different answer to this question, based on its own unique set of geographical, economic or social circumstances. Articulating a vision of an ideal city often necessitates tough choices between competing or even conflicting aims. Nevertheless, one foundational principle remains clear: safety is the foundation of any city, a basic criterion upon which the other characteristics of a successful city depend.

> "CITIES HAVE THE CAPABILITY OF PROVIDING SOMETHING FOR EVERYBODY, ONLY BECAUSE, AND ONLY WHEN, THEY ARE CREATED BY EVERYBODY."
>
> **Jane Jacobs,**
> **Urban Theorist.**

SAFETY: THE FOUNDATION OF ANY CITY

Recognizing the need to prepare for the future, mayors and city planners have often discussed the need for "smart" or "resilient" cities; cities that are highly livable, while remaining eco-friendly and sustainable, enabled by the embrace of the latest technologies. While these overlapping buzzwords contribute important concepts to our understanding of what cities of the future should be like, they all point to the underlying issue of ensuring safety for those who reside there.

Regardless of a city's aspirations to be smarter, more sustainable, eco-friendly, resilient or livable, it needs to be safe first. Without safety as the foundation, any city will face challenges in scaling greater heights.

Without a sense of personal and property security, institutions and businesses cannot function and society cannot flourish. Ensuring that citizens feel safe is a multidimensional task, requiring governments to take a long term and broad perspective. The main challenges that all governments face are providing effective border control and law enforcement for both physical and virtual crime, as well as preparing for disasters, whether they be natural or man-made.

KEEPING CITIZENS SAFE

IDENTITY MANAGEMENT IN A BORDERLESS WORLD

According to the International Air Transport Association's 2013 annual report, nearly three billion people and 47 million metric tons of cargo were transported by air in 2012, supporting 57 million jobs and US$2.2 trillion in economic activity. Clearly, international flights are now an indispensable part of the global economy, strongly incentivizing countries to improve the flow of both people and cargo across borders. However, increased ease of travel has also made borders much more porous than before, as legacy systems struggle to keep pace with the growth in passenger numbers. In-country migration also continues to move large volumes of people from state to state, resulting in growing traffic throughout the country.

At the heart of managing the movement of people is the issue of identity. An efficient border control system is needed to rapidly and accurately assign the correct identity to each person, determining whether he or she is a threat to the country or an innocent traveler. Border control systems also need to be able to cope with extremely high and variable passenger loads, which tend to fluctuate seasonally.

The failure to secure borders could have disastrous consequences. Nowhere has this been better exemplified than in the world-changing 9/11 terrorist attacks, where 19 hijackers slipped past border control officials and security agents to commandeer four planes to their destruction. Apart from terrorist attacks, tighter border control measures are also needed to combat illegal activities such as drug and human trafficking.

However, current security measures are still time-consuming, error-prone and largely dependent on human security personnel. Heightened security at major international airports around the world has made hours-long snaking queues the norm, and travelers have resigned themselves to invasive security checks intended to separate the wheat from the chaff. Governments need to find a way of increasing the speed of border control clearance without compromising on the reliability of their processes, a considerable technical challenge to even the most sophisticated law enforcement agencies.

TACKLING BOTH PHYSICAL AND VIRTUAL CRIMES

While city dwelling confers benefits such as better policing and closed circuit television (CCTV) monitoring of public spaces, population density is also positively correlated with crime rates. According to a 2011 study by the UN Office on Drugs and Crime (UNODC), the most densely populated areas had the highest homicide rates, with homicide rates increasing as a function of population density.

In addition to homicide, overall victimization for a number of different crimes is increased in urban environments. For example, inhabitants of densely populated areas in European Union countries were found to be more than twice as likely to experience crime as inhabitants of intermediately populated areas, and almost three times as likely to experience crime compared to those living in sparsely populated areas. The failure to tackle crime can hinder or even completely paralyze the economy. In Kingston, Jamaica — where 2013 murder rates have seen a 9% hike compared to 2012 — high rates of violence have brought their once thriving tourist sectors to a standstill.

Aside from physical crimes such as homicides, governments increasingly have to contend with virtual or cyber crimes. The Internet has become an indispensable part of everyday life, as both a means of communication and entertainment. From personal computers to mobile phones and tablets, it is now impossible for many to imagine a functioning world without it. Adopting the Internet and information technologies in general can lead to immense economic growth. The World Bank estimates that a ten percent increase in broadband penetration in low and middle income countries would result in a 1.38 percent in gross domestic product (GDP) growth. Apart from economic growth, the Internet also gives remote communities access to vital services such as education, healthcare and other government services.

Yet Internet use is not without its dark side; cybercrimes have risen in parallel with the explosive growth of Internet users. The 2013 Norton report commissioned by Symantec Corporation found that as many as 38 percent of smartphone users had been a victim of cybercrime in the past year. Globally, cybercrime amounts to US$130 billion in direct costs, including losses due to fraud and repairs.

While nearly all law enforcement agencies report an increasing or strongly increasing number of cybercrime acts, including hacking, identity theft and computer-related production, distribution or possession of child pornography, only the most serious cases are reported. One UNODC survey of almost 20,000 individual Internet users in 24 countries showed that only 21 percent of respondents who had been the victim of cybercrime reported the act to the police. Another UNODC study found that online consumer credit card fraud alone was more than 80 times greater than total police recorded computer-related fraud and forgery in the same country. These figures suggest that law enforcement agencies have yet to confront the true depths of cybercrime.

EXPECTING THE UNEXPECTED

MAN-MADE THREATS

Sustaining a city's population requires the provision of public goods such as power, waste management and transport. These critical infrastructures, quietly operating in the background of everyday life, are essential to the smooth running of a city. Any disruption to these services, as a result of man-made disasters such as chemical spills and train collisions, could bring the economy to a standstill. Accordingly, they are also an attractive target for terrorists seeking to cause chaos; an approach particularly favored by "lone wolf" operatives seeking to maximize the impact of their actions.

At present, security measures to protect these critical infrastructures revolve around creating physical barriers patrolled by security personnel. This is far from ideal, as they introduce considerable errors and oversight, and lead to significant labor costs. Video surveillance systems, complemented by analytical software, are slowly gaining ground in replacing or augmenting human security personnel. However, adoption of video surveillance technology is not yet widespread, hampered perhaps by a distrust of the capabilities of automated systems and reluctance to abandon existing legacy systems.

These days, access to the Internet is increasingly important and can be also considered part of a city's critical infrastructure. Disruption of Internet services could lead to "digital paralysis", as seen in the 2007 attack on Estonia which effectively crippled the entire country. Furthermore, as governments store more and more personal data such as social security details and income information online, it is imperative that the data is not compromised. All these call for better information management systems that are both robust and highly secure.

Increased population density and a high volume of international travel also call for stronger health monitoring and response systems. This need has been demonstrated time and again by global health scares such as the recent Middle East Respiratory Syndrome (MERS) and bird flu (avian influenza) outbreaks. In pandemic situations, contact tracing—which is essentially an issue of identity management—is of paramount importance in containing the spread of disease.

NATURAL DISASTERS

While it may be difficult to predict exactly when a disaster will strike, it is certain that natural disasters are increasing in both frequency and cost. According to the UN report on disaster impacts for 2000 to 2012, 1.7 million people died in disasters, and an estimated US$1.7 trillion of damage was sustained.

As the human population continues to grow and make further demands on existing natural resources, the resulting climate change might exacerbate the frequency and severity of future natural disasters. A 2013 study by insurance provider Swiss Re estimates that up to 864 million people will be affected by floods, earthquakes, storms and tsunamis in the near future. The UN Office for Disaster Risk Reduction (UNISDR) considers a high degree of urbanization to be a risk factor for more severe disaster outcomes. However, greater risk exposure need not mean greater vulnerability, as much depends on how cities are managed.

Disaster risk management is especially important for cities. The 2011 Great East Japan earthquake and the subsequent Tohoku tsunami severely tested Japan's highly advanced warning system, seawalls and evacuation plans. The tragedy cost an estimated US$150 billion and took 18,000 lives, or four percent of the population located in the inundation area. In contrast, the 2004 Indian Ocean tsunami resulted in over 20 percent fatalities in the inundation area. While no technology or plan can completely prevent a disaster from happening, Japan's disaster preparations nonetheless can be said to have saved the lives of many and limited the extent of damage done.

Apart from protecting human lives, anticipating disasters and taking preventive measures could also result in substantial savings. A study of flood prevention measures in Bangladesh from 2004–2008 concluded that approximately US$40 was saved for every dollar invested in the regional forecasting and warning system. Similarly, communities in the Democratic Republic of Congo on a small-scale water management project in the late 90s saved US$46 for every dollar invested by the humanitarian agency USAID. In addition, the efforts of the project participants managed to reduce cholera prevalence by 90 percent.

FROM SILOS TO EXEMPLARY PUBLIC SAFETY

Figure 1. S.A.F.E. Framework

Using the S.A.F.E. Framework, we can assess the current status of a city's public safety in four phases: Silo, Advocacy, Fortified and Exemplary (Figure 1).

Cities in the **Silo** phase category are usually plagued by budgetary issues, or lack of focus on public safety initiatives. These cities would already have organized border control services to manage traffic in and out of the country, but typically do not have the infrastructure within the city to push for sophisticated public safety initiatives. The lack of infrastructure and technological advancement means that most safety initiatives will rely on manual manpower. This leaves the city extremely susceptible to damage caused by natural and man-made crime. The lack of actionable intelligence to aid first responders also means that multiple agencies are unable to work in an efficient manner.

The **Advocacy** phase marks the beginning of a new era in public safety for the said city. City planners are now aware of the need to ramp up public safety efforts, and advocate new ways of tackling rising crime rates. This phase will usually see basic video surveillance technologies being deployed in key areas within the city, along with the upgrading of fingerprint solutions to face recognition solutions. More public safety solutions will trickle into the city, although budgets would still remain a main obstacle. Communication between agencies will still remain low as most of them embark on their own direction. It should also be noted that with many agencies pushing for public safety technologies, the lack of a unified approach in the procurement process may result in scattered, overlapping or redundant implementations.

In the **Fortified** phase, public safety has become a priority for city planners, allowing for the implementation of cutting edge technologies. As the city grows, physical security concerns will be managed efficiently by fast-improving first responders due to availability of technologies like digital sensors. Non-physical security will begin to grow in importance as vast amounts of data begin to flow through the city. This means that the city will expand on its focus to cover areas like Cyber Security and Inter-Agency Collaboration.

In the **Exemplary** phase, the city's security operations are mostly automated by now due to cutting-edge Inter-Agency Collaboration technologies allowing for split-second actionable intelligence. Physical and cyber layers achieve similar levels of security as data fusion technologies bring out the best of both worlds. This allows the fully optimized first responders to deal with all kinds of threats effectively and efficiently. City decision making in regards to public safety becomes more centralized as countless agencies now work in tandem with one another.

Figure 2. S.A.F.E. Framework

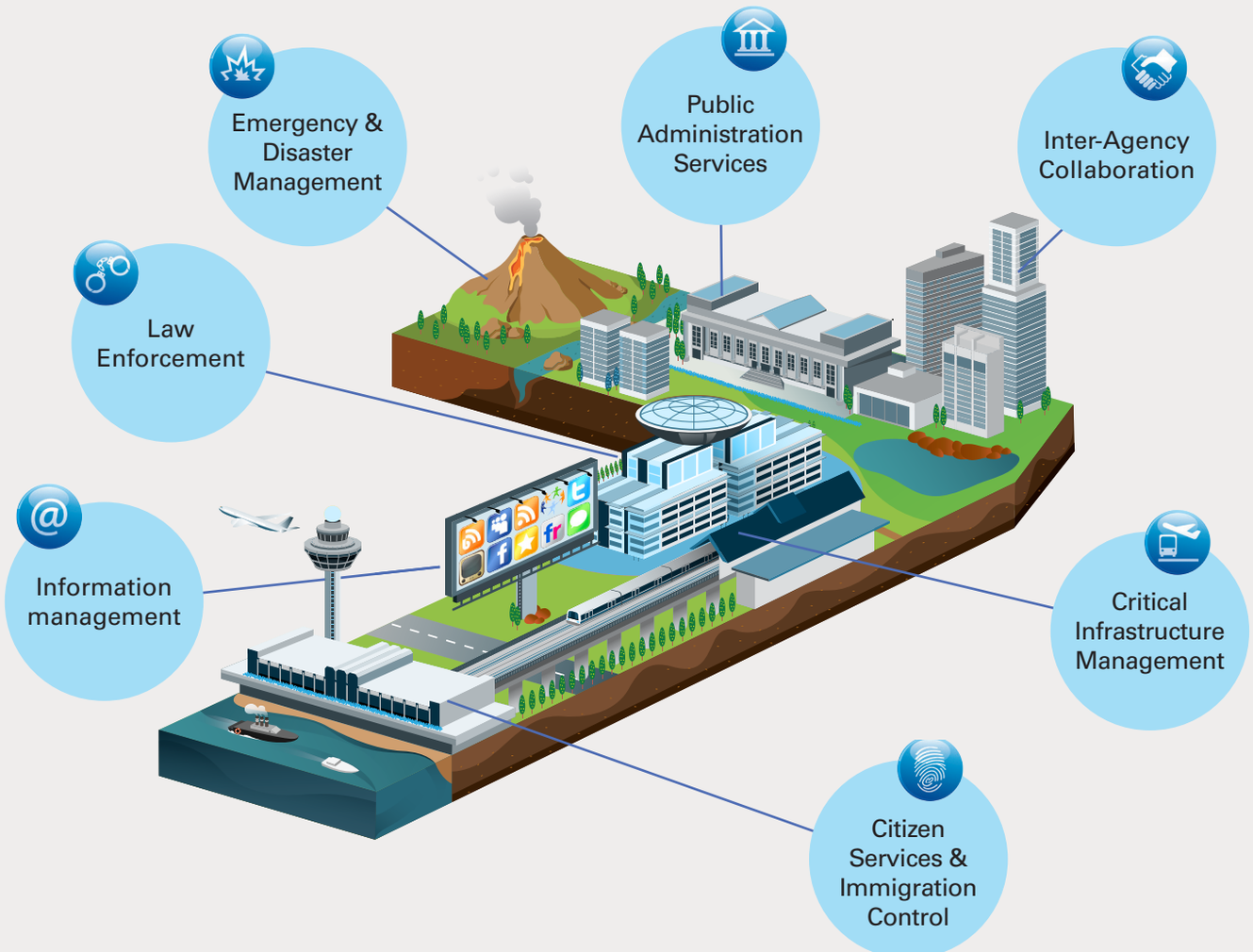
Safe City Stages				
Adoption of 7 Pillars	**Silo**	**Advocacy**	**Fortified**	**Exemplary**
Citizen and Immigration Services	Organized	Organized	Advanced	Advanced
Public Administration Services	Minimal	Organized	Advanced	Advanced
Law Enforcement	Minimal	Organized	Advanced	Advanced
Information Management	Minimal	Minimal	Organized	Advanced
Emergency and Disaster Management	Chaotic	Minimal	Organized	Advanced
Critical Infrastructure Management	Chaotic	Minimal	Organized	Advanced
Inter-Agency Collaboration	Non-existent	Non-existent	Minimal	Advanced
Characteristics	Lack of infrastructure. High damage from natural and man–made disasters. City lacks budget for public safety initiatives.	Beginning to see the importance of public safety. Advocate new methods of tackling crime. Lack of unified direction may lead to unoptimized application.	Physical security concerns will be managed efficiently by fast-improving first responders due to availability of new technologies like sensors. Non–physical security will begin to grow in importance as vast amounts of data begin to flow through the city.	City's security operations are mostly automated. Physical and cyber layers achieve similar levels of security as data fusion technologies bring out the best of both worlds. City decision making on public safety becomes more centralized.
Key Technologies	Fingerprint, AFIS Systems	Face Recognition, Video Surveillance	Sensor Technologies, Cyber Security, Behavioral Detection	Cyber Security, M2M Communication, Big Data, Intelligent Surveillance, Geographical Information Systems

SEVEN KEY PUBLIC SAFETY AREAS FOR EVERY CITY

Ensuring safety is a multifaceted and complex issue, requiring the collaboration of many agencies and the application of many different technologies. Furthermore, each country will necessarily have to develop their own solutions, tailored to their specific context and needs.

Nonetheless, there are several key areas which are consistently seen as the basic ingredients of safety. They are: citizen services & immigration control, law enforcement, critical infrastructure management, public administration services, information management, emergency & disaster preparedness and lastly, inter-agency collaboration (Figure 3).

Figure 3. Seven key public safety areas



PINPOINTING IDENTITIES

with Citizen Services and Immigration Control

Opportunities and threats alike thrive in today's globalized world. Air travel is now ubiquitous and millions of people move across borders each day. Border control agencies must deal with a high volume of human and goods traffic across checkpoints every day, Countries need to secure their borders, ensuring that undesirable elements are kept out while creating a pleasant experience for business or leisure travelers.

Immigration is one area where advanced biometric systems can be used to enhance border security and the speed of border control clearance. Citizens can be enrolled into national identification systems by providing their iris and fingerprint scans for future identification at checkpoints. Airport such as Singapore Changi Airport and Hong Kong International Airport have already implemented fingerprint scanning technologies to facilitate clearance of travelers.

Apart from national identification, governments have been placing strong emphasis on voter identification. Fast and accurate verification of each voter's identity on Election Day is vital in managing large crowd volumes. With the employment of biometrics and centralized voter ID databases, election fraud can also be prevented.

Case study: South Africa's Home Affairs National Identification System (HANIS)

The Challenge

South Africa's population of 48 million depends on government issued identity booklets for access to public services and daily transactions. The legacy paper-based system relied on manual authentication of fingerprints, a time-consuming and laborious process.

The Technology

In order to transition to a digital database, the South African Department of Home Affairs turned to NEC's Automated Fingerprint Identification System (AFIS). Trusted by governments around the world, NEC AFIS is trusted and used by many governments around the world.

The Benefits

More than 30 million records have been successfully transferred to the Home Affairs National Identification System (HANIS).The system has reduced waiting times while enabling up to 70,000 searches per day. Furthermore, the accuracy of the system also provides robust protection against fraud and identity theft.

COMBATING CRIME

with Law Enforcement

The safety of a city is a significant consideration for both individuals and businesses alike. However, crime tends to increase as cities grow. The challenge for governments is to ensure that citizens feel safe while continuing to enjoy the benefits of city life.

Biometrics technologies can be used in authentication, by establishing the identity of an individual who has access to a secure facility. Fingerprint scans can be used to protect sensitive or personal data in notebook computers and mobile devices from unauthorized access. If a crime has been committed, suspects can be identified by scanning facial images from a video taken at the scene of the crime against a database.

Case study: Pennsylvania Justice Network

The Challenge

The Pennsylvania Justice Network (JNET) is an online environment that allows law enforcement agencies and state offices to access criminal justice information. The heritage system had labor-intensive data entry methods and cumbersome user access. More importantly, it had outdated facial-recognition technology with low matching accuracy.

The Technology

NEC's patented facial recognition system, NeoFace®, and DataWorks Plus' FACE Plus integrated facial recognition system were selected to overhaul JNET.

The Benefits

NEC analyzed the existing database of over 3.5 million criminal booking photos and devised a customized algorithm for JNET. This resulted in faster, more accurate identification matching that had the ability to work with poor quality and low-pixel count images. The JNET Facial Recognition System received Laureate and 21st Century Achievement Awards from International Data Group's Computerworld Honors Program in 2012.

SAFEGUARDING VITAL INSTALLATIONS

with Critical Infrastructure Management

Providing robust electricity, water and transportation services are the mandate of any city planner. These essential services keep society running behind the scenes. But threats may come from anywhere, requiring constant monitoring and surveillance. It is here that automation can make a significant impact.

Technologies including video analytics and monitoring systems can provide reliable and sensitive protection. These automated systems can improve the speed and accuracy of threat detection while lowering staff and equipment cost. Both offline and real-time meta-analysis methods can also help identify previously blacklisted subjects. Not only are these technologies used by governments, but industries such as oil and gas also rely on them to secure important assets and operations.

Case study: Train video surveillance

The Challenge

The 2005 London train bombings highlighted the fragility of public transport systems and exposed the inherent risks onboard trains and buses. The Yishun mass rapid transit (MRT) bomb plot uncovered in 2001 showed that even relatively safe Singapore was not immune to the risk of terrorist attacks.

The Technology

To improve safety across Singapore's MRT system, NEC has been selected to provide video surveillance for all existing lines.

The Benefits

Slated for completion in 2018, the video surveillance system provides real-time monitoring of train operations and is expected to assist law enforcement agencies in even reconstruction. The system can also be adapted for future needs, to include voice recording and video analytic capabilities.

PROTECTING PUBLIC SERVICES

with Public Administration Services

Governments are increasingly moving many of their services online for a number of reasons, including increased convenience for its citizens, better transparency and cost efficiency. As the government holds sensitive personal information such as tax information and national identification numbers, the move to e-government needs to be accompanied by enhanced security measures.

In addition to virtual risks, governments also need to protect their populations from disease outbreaks resulting from an increased population density. As seen in recent outbreaks of bird flu and SARS, infectious diseases can cripple countries, exacting a high toll on human health and the economy. If a pandemic should strike, the spread of the disease can be contained by tracing individuals who have been exposed to the infection, and swiftly placing them under quarantine.

Case study: Argentina's Autopista de la Informacion

The Challenge

Access to government services can differ widely in Argentina, with rural residents often missing out on health, education and social security benefits enjoyed by city dwellers. In the province of San Luis, where more than 80 percent of the population lives in widely spread rural communities with little access to electricity, three hour bus rides to the city to make a medical appointment are common.

The Technology

In an ambitious plan to provide telephony and internet services to every community of twenty or more citizens, the Argentinian government partnered NEC to launch the Autopista de la Informacion, or information highway. NEC provided a fully integrated system, including actual infrastructure of optical fiber, radio and satellite links as well as a secure data center and specially developed software solutions.

The Benefits

Citizens in remote regions that did not even have electricity now have the same access to government services and information as city dwellers, narrowing the digital gap between the rich and the poor. For example, they are now able to make medical appointments in city hospitals online, saving them from time-consuming travel.

ENSURING DIGITAL SAFETY

with Cyber Security

As more and more people and devices join the Internet, the number of potential targets for cybercrime increases. The world is also moving towards an "Internet of things", where objects such as appliances, vehicles, power and water meters or medicines are assigned an Internet protocol (IP) address. Big data analytics can help governments collect and make sense of the large volume of data that inundates the cyberspace, including publicly available social media feeds.

Governments also need to secure their networks against hacking or virus attacks, which call for more traditional security measures such as firewalls, intrusion-detection sensors and intrusion prevention measures. They will also need to address privacy concerns, especially when social media analytics is concerned, which is why good data governance practices must be built into the system from the very beginning.

MITIGATING CATASTROPHES

with Emergency and Disaster Management

No city is immune to disasters. Even regions fortuitously protected from earthquakes and volcanoes could face natural disasters such as hurricanes, floods and tsunamis or man-made disasters such as train collisions or terrorist attacks. In the event of an emergency, pre-existing preparedness measures and the rapid execution of post-emergency plans could make the difference between life and death for those affected.

Governments must quickly collect information, process it to reach an optimal response, and disseminate the decision. Sensors such as surveillance cameras, water level gauges, rain gauges and seismometers can be used to gather information on disasters and emergencies. All these data can be seamlessly integrated at a command center, and then rapidly distributed to the different agencies such as the police, army and hospitals.

ACHIEVING SAFETY THROUGH SYNERGY

with Inter-Agency Collaboration

Many of the challenges that city planners face, ranging from terrorism to natural disasters, require the cooperation of different branches of the government. To launch a coordinated response, different arms of the government, with different levels of access, must contribute their own sets of data input.

Here, technology can be used to facilitate cross-agency collaboration. In the aftermath of a disaster, governments must swing quickly into the recovery stage. Big data, including the latest machine to machine (M2M) communication technologies, promises to enable the rapid response required. Ultimately, the goal of the inter-agency collaboration framework is to achieve situational awareness, a multifaceted understanding with reasoning capabilities that not only displays information but presents actionable intelligence.

Case study: The Safe City Test Bed in Singapore

The Challenge

Singapore has sought to harmonize various arms of the government, ranging from emergency services (Singapore Police Force, Singapore Civil Defense Force) to environment management (National Environment Agency), utilities (Public Utilities Board) and transport (Land Transport Authority).

The Technology

In 2013, a consortium led by NEC Asia Pacific was one of the four selected to develop the Safe City Test Bed in Singapore. NEC's proposition is to build a complete, end-to-end framework that uses technologies such as advanced data analytics, risk analysis and relationship modeling to allow agencies to integrate disparate information from various sources.

The Benefits

NEC's solutions are expected to help the different agencies to overcome infrastructural and technical barriers to inter-agency collaboration, optimize the use of manpower, and improve situational awareness and anticipation of security threats.

NEC PUBLIC SAFETY

As the urbanization of the world continues at breakneck pace, cities everywhere are experiencing growth in both size and complexity. Each city has a unique set of circumstances, and city planners must defend against multiple types of security threats: man-made and natural, physical and virtual.

City planners and governments need to find ways to respond to the immediate needs of their citizens, while also sustaining the effect for the long run. Here, selecting the right technology can play a significant role in managing potential risks, ultimately making cities safer. City planners must therefore seize the opportunity and confront security challenges before problems arise.

To keep cities safe, NEC has developed a comprehensive suite of public safety solutions in the areas of national identification, law enforcement, immigration, emergency and disaster response, and protection of key physical and cyber infrastructure. NEC's biometric identification systems, for example, are used by more than 500 customers in over 40 countries to protect and verify identities.

While it may be impossible to anticipate every eventuality, it is prudent for governments to plan for adverse events. To help agencies work together, NEC has introduced technologies that enhance inter–agency collaboration, breaking down silos and strengthening teamwork. NEC has also helped governments develop early disaster warning systems and robust emergency response protocols, including command and control centres. In situations of national importance, technology can play a crucial role, allowing city authorities to quickly take stock of a complex situation, and respond in an agile and timely fashion.

Cities of today that are effective at responding to threats and disasters will enjoy robust growth and peace for decades to come. NEC has the experience of working closely with city planners around the globe, and we are committed to developing solutions that are tailored to the local context. Whether a city is looking to find ways to improve its emergency response capabilities, defend against physical or virtual threats, or use its energy resources more wisely, NEC can help. By offering a holistic suite of solutions that address issues of all complexity levels, NEC is here make cities safer.

"NO URBAN AREA WILL PROSPER UNLESS IT ATTRACTS THOSE WHO CAN CHOOSE TO LIVE WHEREVER THEY WISH."

Jonathan Barnett, Emeritus professor of city and regional planning, PennDesign.

REFERENCES

"Mind the Risk: A Global Ranking of Cities Under Threat", Lukas Sundermann, Oliver Schelske, Peter Hausmann, Swiss Re, 2013.

"Extended–Range Probabilistic Forecasts of Ganges and Brahmaputra Floods in Bangladesh", Peter J. Webster, Jian Jun, Thomas M. Hopson, Carlos D. Hoyos, Paula A. Agudelo, Chang Hai–Ru, Judith A. Curry, Robert L. Grossman, Timothy N. Palmer, AR Subbiah, *Bulletin of the American Meteorological Society*, 91(11):1493-1514, 2010.

"Economics of Disaster Prevention: Measuring the Costs and Benefits of Disaster Risk Reduction", Center for Strategic and International Studies (CSIS), 2011.

"Global Study on Homicide: Trends, Context, Data", United Nations Office on Drugs and Crime (UNODC), 2011.

"State of the World's Cities 2012/2013", United Nations Human Settlements Program (UN–HABITAT), 2012.

"Comprehensive Study on Cybercrime — Draft", United Nations Office on Drugs and Crime (UNODC), 2013.

"Hidden Cities: Unmasking and Overcoming Health Inequities in Urban Settings Report", World Health Organization, The WHO Centre for Health Development, Kobe, and United Nations Human Settlements Programme (UN–HABITAT), 2010.

"World Energy Scenarios: Composing Energy Futures to 2050", World Energy Council, 2013.

"The Norton Report", Symantec, 2013.

International Air Transport Association's 2013 annual report

About NEC Global Safety Division

NEC Global Safety Division, a business division within NEC Corporation, spearheads the company's public safety business globally. The Division is headquartered in Singapore and offers solutions in the following domains: Citizen Services & Immigration Control, Law Enforcement, Critical Infrastructure Management, Public Administration Services, Information Management, Emergency & Disaster Management and Inter-Agency Collaboration. Leveraging on its innovative solutions, the Division aims to help government and business make cities safer.

NEC Global Safety Division

Global Headquarters: 2 Fusionopolis Way, #07-01 Innovis, Singapore 138634
For enquiries, please contact safety@gsd.jp.nec.com

nec.com/safety