NEC PUBLIC SAFETY WHITEPAPER

\Orchestrating a brighter world NEC

THE FUTURE OF PUBLIC SAFETY

EIGHT INFOCOMM TRENDS THAT WILL IMPACT BUILD-UP OF SAFER CITIES

WE MAKE CITIES SAFER

Using technologies to safeguard lives and property

Not many people think much of it, but inside the pocket of many urban citizens today is a device that probably packs in more sensors, processing power and connectivity than some of the systems used in emergency response teams.

The smartphone, with a GPS sensor locking on to satellites in the sky, access to the Internet at 4G speeds, and cameras that capture live-feed high-definition video, has enabled citizens to track and find out the latest information, whether this is on traffic jams, subway delays or environment issues such as air pollution.

While information was once a scarce commodity, today's world is filled with easily available data – think of pictures and videos from citizens' smartphones. One daily challenge for city planners and citizens alike is making sense of the information out there.

In a city with thousands of surveillance cameras, can the thousands of hours of video footage be swiftly pieced together in a coherent manner to search for a person, based on his appearance? On the Internet, where social media networks allow citizens to share information – sometimes erroneous information – can city planners make sure the right advisories are put out to the public?

To make things even tougher, citizens often demand faster fixes for emerging problems. Impatience can be easily amplified over social media networks, even while city authorities find out the source of, say, a haze that has blown over a city and rush to provide the correct health advisories to people.

These are the challenges. Yet, they also open up opportunities.

There are solutions, for example, in facial recognition that uses neural networks, which can help "recognise" a face from a crowd in a video. This helps identify persons of interest faster and more accurately than most other systems.

Social media, too, can be harnessed as a form of ground-up activism as city authorities find solutions to a crisis after a natural disaster. Sometimes, that citizen on the ground with a camera can provide a good description of what happened or is happening. He can mark out places on a map, such as a working petrol station, during a flood.

Increasingly, in inter-connected cities, infocomm technologies empower new nerve centres that are necessary to keep things ticking, solve complex problems and create situational awareness for various agencies. More importantly, they ensure that vast amounts of data collected through the various technologies previously mentioned flow fluidly throughout the entire city, bringing relevant agencies together and ensuring that they collaborate as a well-oiled machine.

As cities become larger and the world becomes less predictable, an unprecedented convergence of key technologies in recent years has also helped bring a futuristic vision of a safer city closer to reality.

Whether this is in the form of Big Data that discovers actionable information from across various government agencies, or software-defined networks that enable networks to adapt and work with one another seamlessly to provide information to users who need it, the future looks very promising with new solutions that are beginning to see real-world usage.

At NEC, we have spent more than 30 years working with governments and city authorities to design and roll out systems that take advantage of infocomm technologies to transform the lives of citizens.

With solutions ranging from immigration control to emergency and disaster management, we have helped establish safer cities for more than 480 customers in over 30 countries, in Asia-Pacific, Latin America, Europe and the United States.

Many governments have already taken the first step of setting up a digital fingerprint identification system, so they can provide services to citizens more easily. Identification also helps reduce election fraud, ensuring true people's representation in democracies.

Going a step further, many leaders are looking to install smart sensors to better detect the "vital signs" of a city, so they may have the necessary information to make better decisions.

A sensor that measures and provides real-time updates on wind speed, for example, can tell planners how a contagion may affect people at risk. A network of such sensors, set up as a system of systems, an "Internet of Things", can provide vital situational information for planners to make critical decisions.

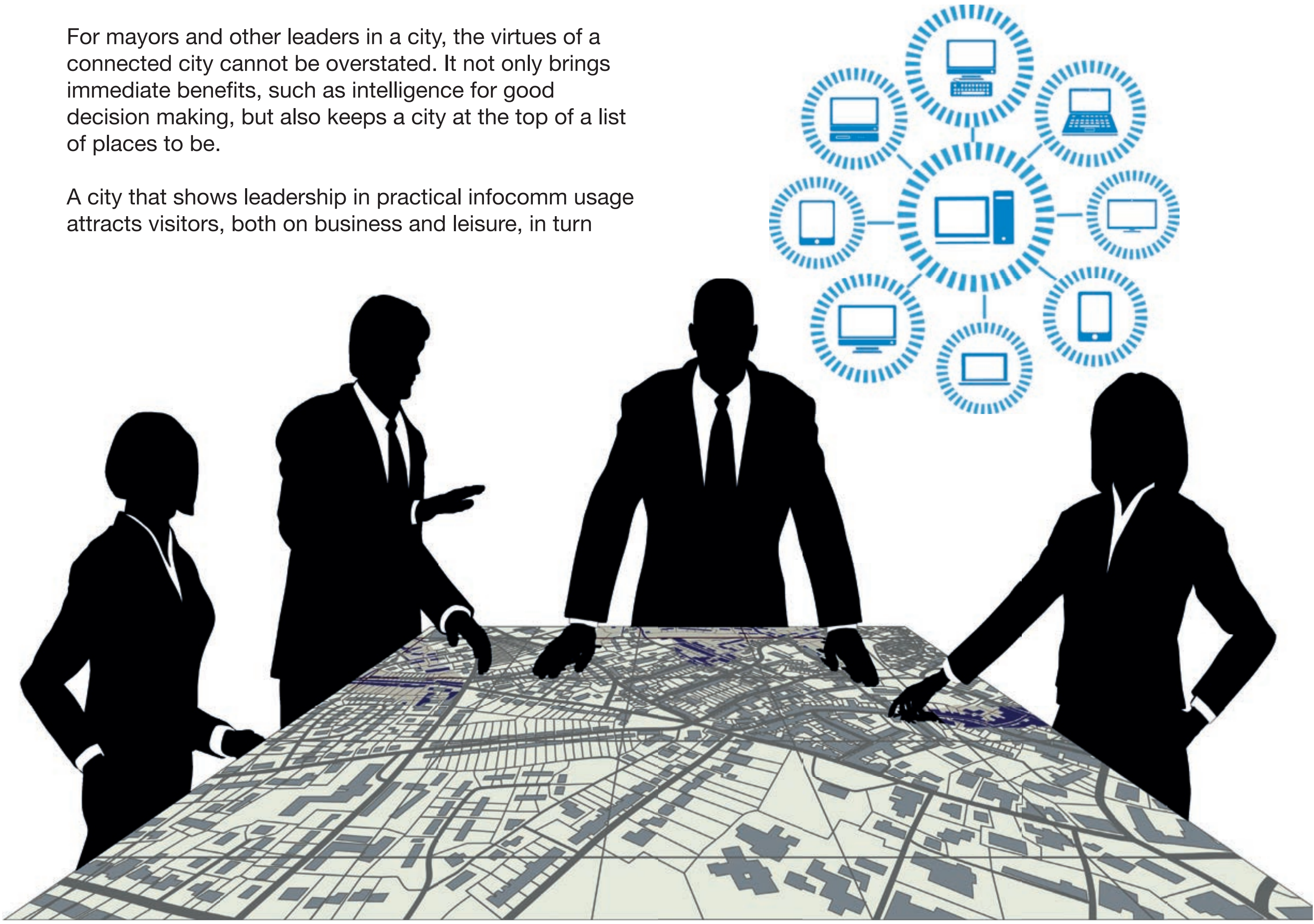
For mayors and other leaders in a city, the virtues of a connected city cannot be overstated. It not only brings immediate benefits, such as intelligence for good decision making, but also keeps a city at the top of a list of places to be.

A city that shows leadership in practical infocomm usage attracts visitors, both on business and leisure, in turn bringing more vibrancy to the city. Singapore is one great example. At the centre of East and West, it is also very well connected with fibre broadband networks, and boasts a lively start-up scene that enables developers to use the country to test the latest technologies.

Surely, technology alone does not solve problems. That takes leadership, foresight and political will. As technology advances, citizens too have to be comfortable with the privacy issues involved in data being collected, shared and processed by the relevant authorities.

Ultimately, governments and city authorities will have to evolve in their planning and decision-making, as cities become bigger and the world we live in becomes more multi-faceted and unpredictable. The advent of inter-agency collaboration - a once fleeting concept which is fast becoming a reality due to rapid advancements in technologies like Big Data and Machine-to-Machine Communications - will do well in driving all parties towards stronger cooperation within the very near future.

With the right innovation tools, city planners can build capacity and translate all the information coming through their feeds into action. Eight key technology trends in the coming years will shape such efforts to integrate infocomm into safer cities.



1. Smart Sensors

In the years after the September 11 terrorist attacks, governments around the world have been deploying thousands of cameras to capture videos of street corners, common walkways and other places of interest.

The issue that many law enforcement agencies face now is not so much a lack of data but often too much of it. Opening the data flood gates without being prepared for the volume of data often means being drowned in it. Too much information can overwhelm rather than help.

In the short time span that authorities have to, say, identify the recent Boston bomber, they will have had to look through thousands of images to find a person of interest.

What can assist here are smart sensors that not only provide plain video but also GPS location information, for example. Better still, if a video analytics system can recognise facial patterns and zoom in to look for a particular facial feature on a suspect. This has to be both accurate and fast.

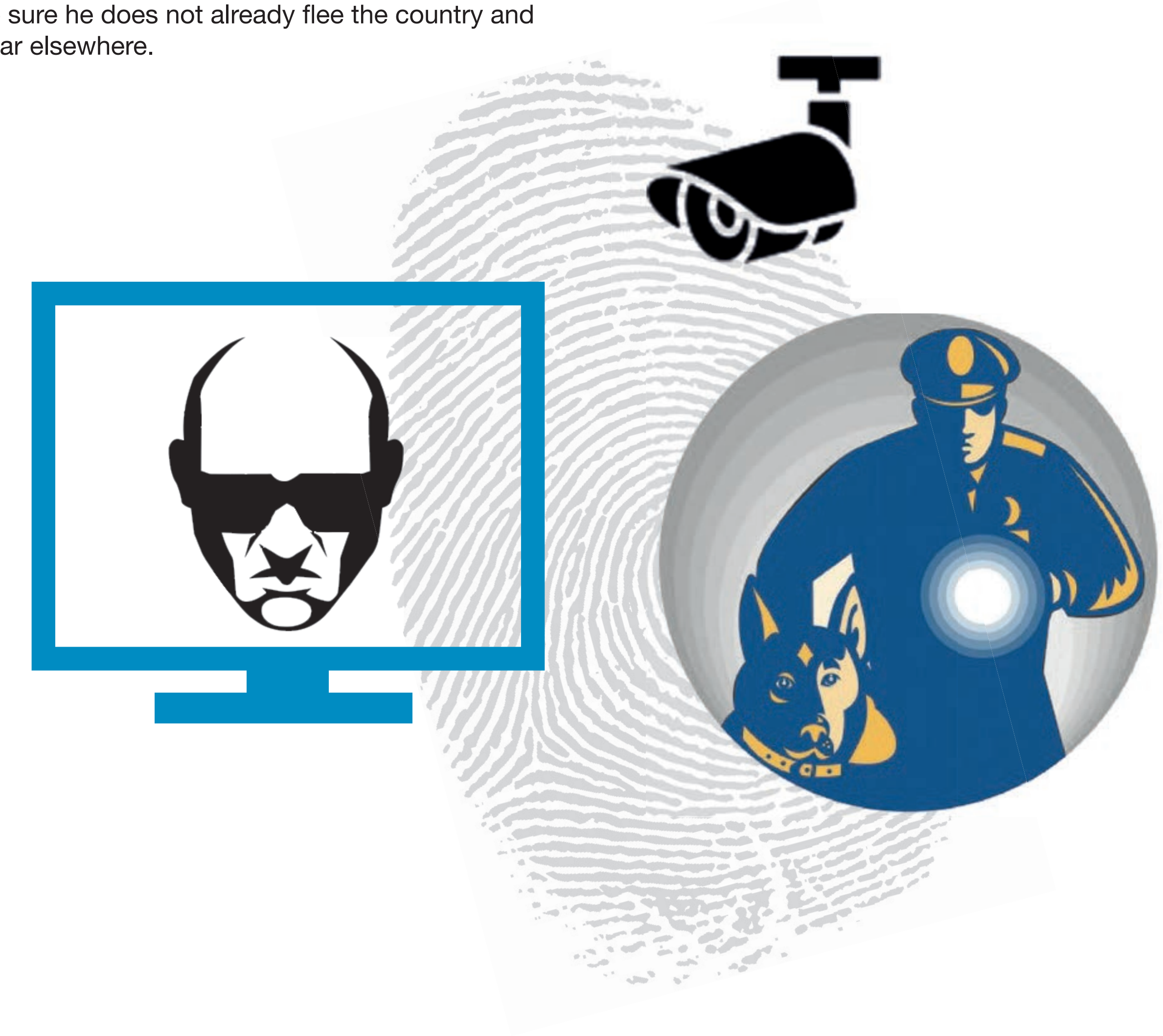
Indeed, the success of many law enforcement efforts will be down to how fast and how well they can process the data in front of them. In the aftermath of a terrorist attack, the authorities will have to identify a suspect quickly and accurately, sometimes in hours or days, to make sure he does not already flee the country and disappear elsewhere.

The scope extends beyond video cameras. As the eyes and ears of a smart city, other sensors that measure wind speed and direction, quality of water in a reservoir and air pollutants are just as vital. To qualify as "smart", these sensors have to connect, in real-time, to a city's nerve centre, providing timely information for both citizens and city planners alike.

Current systems often rely on cellphone networks for one-to-one links, which may saturate during a time of crisis, especially if citizens are frantically trying to communicate with one another. Various new solutions are now proposed, using new wireless spectrum or perhaps building a separate Internet of Things dedicated to machine-to-machine communications.

Whatever the delivery system, one thing is certain. The huge amounts of information will have to be better processed. "Brute force" forensics will not work, going forward.

Instead of sieving through everything without a clear idea of what to search for, city authorities will have to invest in knowledge management and advanced analytics to prepare for incidents where they have to make sense of huge amounts of data in a very short time.



2. Big Data

If smart sensors bring loads of information to public agencies, then the idea of Big Data is to make sense of it by analysing for patterns and understanding the relationships between various items in a data set.

Abundant, on-tap storage and number crunching computing power have made this possible today. Yet, the idea that one can throw a pile of data into a machine and discover accurate trends and predictions from it is not only flawed but dangerous. It leads to assumptions and fallacies that can lead to poor decision making.

To be sure, Big Data can help government agencies in many ways. One area is public safety. Data collected over the years – "long data" – can help in an assessment of how secure an installation is, based on threats and risks.

Another area concerns digital crime. Big Data can provide advanced analytics of how, where and when hackers may attack a city's critical cyber infrastructure. By providing forewarning, city authorities can be more proactive in preventing an attack.

Yet, Big Data is not the simple answer to many issues that city planners face. Often, the theory and the ground situation can be very different.

Government planners have to be wary of vendors keen to supply more computing hardware and software systems, and be more focused on a holistic, multi-disciplinary approach when it comes to adopting Big Data in their decision-making process.

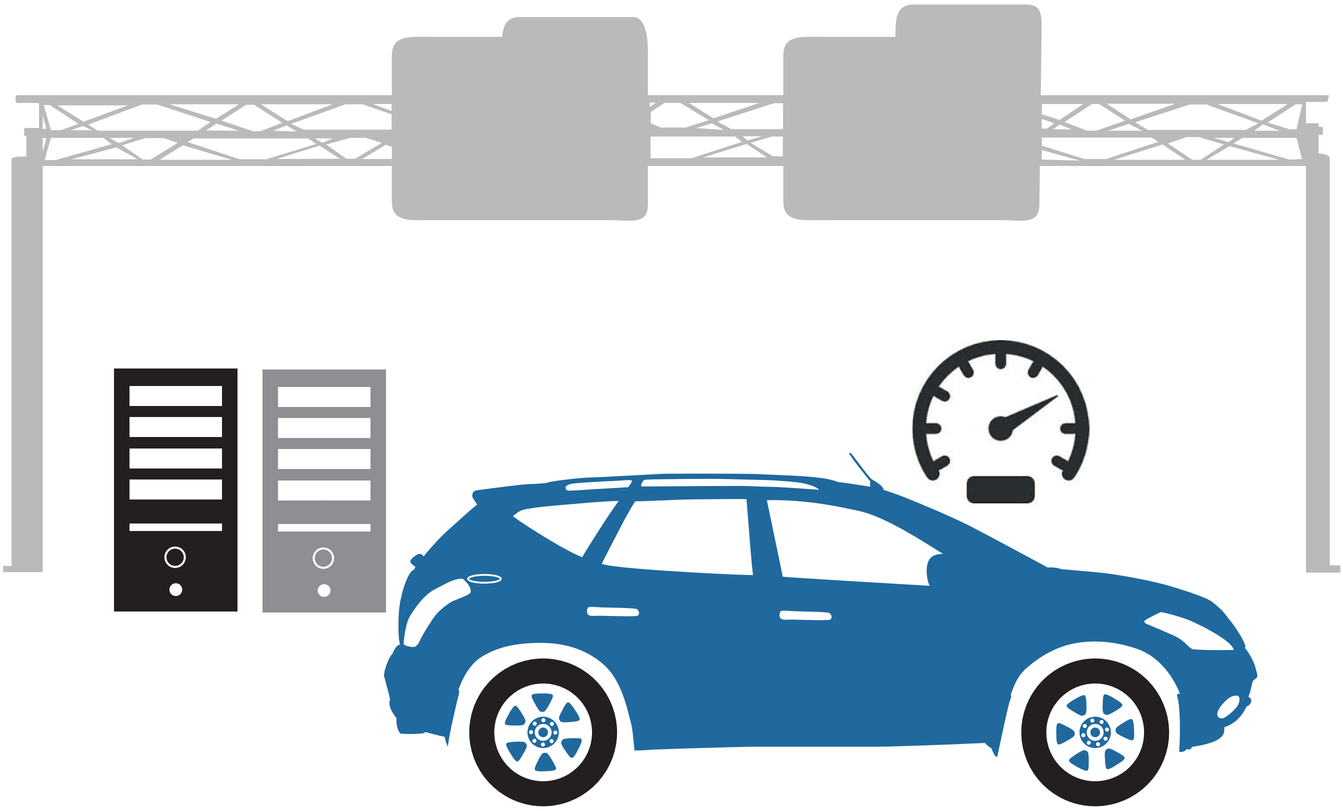
One simple question to ask is whether a Big Data solution provider uses relevant data sets and big-enough sample sizes. Traditionally, statisticians follow these rules, and so should any data that is input into a system to find new trends and predictions.

Very often, despite the huge amounts of computing data and information available at hand, the most accurate results still require domain experts who know how to search for the right things in the right way. Without that, Big Data merely throws up random results, which can vary differently each time a test is run.

Where can governments find useful, relevant data? This is where information management and inter-agency collaboration systems come in. They make it easy to manage, resolve and make use of the data collected from each government agency.

With a smart strategy for handling data, governments will not find themselves overloaded with information, or using the wrong sets of information to base a Big Data query on. Trends and predictions will also tend to be more accurate, leading to better decision-making.

3. Machine-to-Machine Communications



Data doesn't just come from one source, or come in one direction. Much of the massive amounts of data in future will likely be collected by smart devices – machines – that talk to one another. The communications among these machines is now a key consideration in developing smart cities.

After all, machines are going to communicate a lot more among themselves in future, often without any human intervention. Today's Internet servers already talk to one another all the time. In the physical world, this will become even more common.

Many smart sensors will be able to not just communicate to a central system but also connect to their peers. Like how insects act in a swarm, dozens, hundreds or even thousands of sensors can interact with one another to relay information, verify that data and ultimately present a coherent piece of information to human decision-makers.

One application is in future cars and road systems. Already trials are being conducted in Europe and elsewhere, where cars can be outfitted with communication devices that announce their presence as well as "talk" to surrounding devices, such as those installed on the kerb or on a traffic light.

A very fast, split-second change in a situation, say, if a driver is running a red light, could trigger a warning in other drivers in the vicinity, so that they are warned of the imminent danger.

Such systems can also help alleviate jams. Each device could, for example, connect to one another when many cars are stuck on a highway jam, to relay that information all the way back to drivers who might be heading towards the jam, so they may avoid it.

Such intelligent agents are expected to be common in future cars, and NEC is a major vendor involved in several trials of such smart cars in Europe. Though such technologies are still some years away from mature commercial rollouts, issues are being ironed out to bring the scenario to reality.

Machine-to-machine communications will impact many facets of urban life. Its effect will become more pronounced as cities become denser and interactions between not just humans but an increasing array of sensors and communications devices increase.

Among the potential issues that government agencies have to work out is that of identity management. They would have to ensure that each machine on the network is what it says it is, so there is no "fake" information being spread through a swarm of machines.

The timely arrival of cross-agency collaboration solutions will manage challenges ranging from data security to information dissemination within huge pools of machines residing in various locations under different establishments.

4. Wearable Computers

Among the "machines" that communicate to one another all the time would be ones that we put on our bodies as we go about our day.

Once thought of as futuristic toys, wearable computers are a reality today, thanks to low-cost electronics and connectivity to on-demand resources on the Internet. From sensors that track your evening run to the state-of-the-art Google Glass that provides a full augmented reality view of the physical world, wearable computers are set to play a key role in public safety in future.

Law enforcement and public safety officers can be fitted with eye glasses that automatically provide them with real-time information that could save lives.

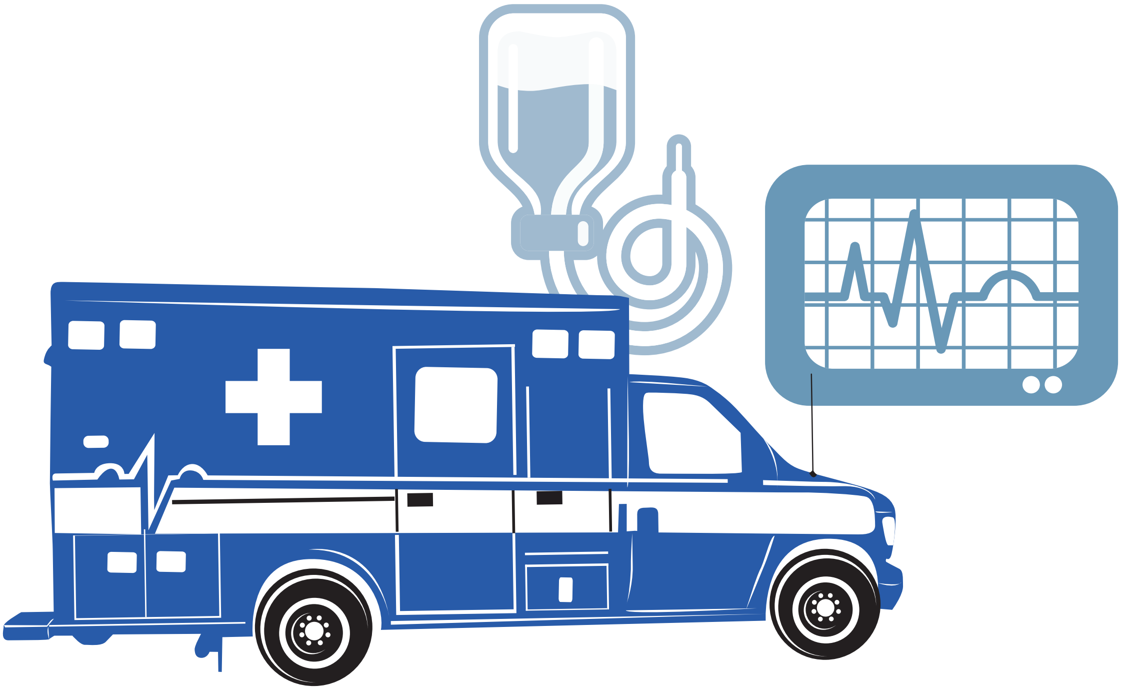
A police officer can carry out a background check on a person instantly without looking up his laptop in the patrol car. Similarly, he could be warned that a criminal is on the loose near his location, without having to wait for confirmation over the radio. He can even be guided there visually.

The same applies for ambulance crew, who may be given the important health statistics for a patient that they are rushing to the hospital. The wearable computer on the officer can assist him in making critical decisions on how to treat the patient in an emergency.

Many things have to work together for this to be an ideal scenario. For starters, wireless networks that feed information to the wearer have to be robust enough to handle real-time information. A first responder to an emergency should not have to wait for data to download onto his wearable computer.

What about the recordings that law enforcement officers have stored on their wearable computers? How can the judicial system properly ensure that videos of a crime scene are correctly handled as forensic evidence? The answer could be in the shape of an information management system tailored to fit law enforcement requirements.

The biggest challenge, obviously, is not just in the technology. Users have to be able to get used to the technology. Wearing an eye piece that constantly feeds information may be a chore for some users, so the type of context-aware information that they receive has to be useful.



5. Internet of Things

With so many non-human sensors, meters and even connected eye pieces "talking" to one another, the Internet of Things is one network that can enable these conversations. This network has to be not just fast but real-time, and come with low latency.

This network may be parallel to the wireless networks we use now – 3G, 4G or Wi-Fi – or perhaps a heterogeneous one that can check on the condition of each network and choose the best path through the various networks. Sounds like how the good old Internet works? Well, it is, except the Internet of Things is used by non-human users.

The data exchange may not always require lots of bandwidth, since the information can be a simple data point on wind speed or water level. However, the network has to be robust enough to handle millions of connections with little lag.

How can such an evolved network benefit a city? Besides hooking up wearable computers or environment sensors for regular machine-to-machine communications, one possible application is smart meters.

Can a setup of smart meters that measure, say, the usage of electricity or water, communicate among themselves to relay the reading to utilities providers seamlessly each month, without requiring an officer to check in at each household?

The technology for such an application is already in the works and will become even more sophisticated in the years ahead. The vision is one made possible by a growing Internet of Things that will become more pronounced.

As a sign of things to come, the market for the Internet of Things and related Machine-to-Machine communications is expected to grow to a huge US$290 billion by 2017, up from a modest US$44 billion in 2011, according to a report by Markets & Markets released in July 2013.

How many devices will be connected in this Internet of Things? By 2020, there could be 30 billion, according to ABI Research, or 50 billion, if you ask equipment vendor Cisco. In comparison, there are only going to be 2.4 billion PCs, tablets and smartphones sold in 2013, according to Gartner.

Many aspects still require further thinking, to be sure. For example, how do machines check on one another, since they are expected to trust one another? Can they know when to drop a fake signal?

In implementing a plan for the Internet of Things, governments have to consider the effects of data leakage and viral attacks. And in devising an information management strategy, they have to balance the effectiveness and speed of the network, against the security required to check data packets that are passed through the network.

6. Software-Defined Networks

Perhaps a software-defined network, more flexible, much easier to configure from a central controller, can be part of the answer.

Today's networks are always up, or at least they are expected to. When engineers design a network, they ensure its survivability by locking all doors from unauthorised users. What happens when these users keep banging, until the door breaks down or the house itself is torn apart?

That's exactly what hackers sometimes do with denial of service attacks. By accessing a website through thousands of "zombie" or infected PCs, they overwhelm a network and bring it down. If this is a network providing essential services to a city, millions of people will be adversely impacted.

In future, the game could be shifted dramatically. Can the house – the network – be shifted instead of being always standing upright, subject to attack? Can it be moved somewhere else where it is safe from the repeated, brute force attacks?

Though this is still very new, software-defined networks could one day provide such a solution. When a profile of an unauthorised user comes knocking to ask for entry, the network could identify a potential threat and shut itself down instead of staying up and being prone to further attacks.

Authorised users will then be shifted to access via another, changed, route. This flexibility is possible because networks can be made changeable on the fly, like code on software.

A paradigm shift is required in the building of city-wide networks in future, as networks can be changed to fit the profile of a user in future. Standards are still evolving, but there are interesting opportunities here. Future networks can be made more resilient by being flexible to a situation rather than toughing it out against formidable threats.

As a new field, software-defined networks have enormous potential. Their flexibility can, for example, help enable the most important data communications to get through, despite increasingly congested airwaves loaded with the mobile phone data of millions of users.

Today's public safety networks are often fixed, and use "infrastructure" modes that are hooked up on pre-set radio frequencies. Might software-defined networks, which adapt to the needs of users on the ground, provide a better route over the airwaves, say, when a fixed network is not available?

This could come in handy in disaster areas where the local infrastructure is severely damaged. Software-defined networks could be run on "ad hoc" mode and tap on available public networks such as cellular networks, if these networks provide better bandwidth for emergency workers.

Instead of worrying about which frequency to tune one's radio on, the future first responder will be better off automatically tapping on the best network available.

7. System of Systems

Ultimately, all public safety systems – including human operators, technologies and organisations – have to work seamlessly together for a smart, safer city to function well. Key here is a system of systems approach to building capacity.

One example of this is in the wireless communications that first responders use. With so many proprietary systems in place today, state and local police officers may find themselves unable to talk to one another over the radio, even when they are both physically near a crime scene.

That had been one issue that plagued law enforcement officers in Central Nebraska in the United States. Instead of a top-down approach, where the state would dictate one set of systems, each county came up with its own system. Things were fine as long as they made sure they had a way to interoperate.

For communications, this meant setting up Internet Protocol radio communications and integrated software systems that enable officers from various departments or counties to communicate with one another, share SOPs and achieve greater situation awareness during an emergency.

Indeed, such a system of systems approach is what the US has in mind for in its next-gen 911 infrastructure. Moving away from the simple telephone system used since the first 911 call in 1968, the country aims to connect up various systems using Voice over Internet Protocol (VoIP) as well as enable other data services for emergency responders.

8. Privacy and Governance

As government agencies collect more information, one obvious concern for citizens is privacy. Rather than a feature that is built in after a system has been architected, privacy protection and governance have to be part of the design from the start.

The key challenge is providing each agency the information it needs – instead of having that locked in silos – while assuring the public that only authorised persons are allowed to access that information. As data becomes more ubiquitous and data mining becomes easy, governance is key for city planners.

No matter how advanced a city is, the first step to securing private data is critical. Developing an information management strategy from Day One will enable governments to clearly define its priorities while weighing up the concerns of the population it serves.

Government regulators also will have to define new roles as new issues emerge. For example, if a malfunctioning sensor reading from a future motorway kerb causes a big crash on the motorway, who is to blame? Investigators may have to find out if this is due to the sensor company or the vehicle manufacturer that failed to analyse data from other sources and instead relied on one specific information, which failed this one time.

By rolling out a new network that could change the way motorists react on the roads, government agencies first have to ensure the system doesn't add to any potential issues with liability. It has to work and work well for citizens before rollout.

And since the impact of such technologies can be both deep and widespread, clear regulations have to be set in place by government regulators, before the technologies are rolled out. They can still build enough flexibility into these regulations, so that the rules can evolve with the technology, but they also have to be clear where responsibility lies. The role of regulatory authority is important to set the demarcation between what humans will do and what machines will do.

Towards Safer Cities

Clearly, infocomm technologies are at the heart of safer cities in the future. In building safer, more liveable cities, planners will have to identify which of the key trends and issues are topmost on their agenda. Each city varies from the other, but there are common experiences to be shared and learned from.

For city leaders and planners, this may be a time to consider the following actions, as plans are drawn up for the development of a safer city:

A **Conduct a quick audit of the systems and projects in place currently. This will bring clarity to the systems – or lack thereof – in place today, so planners have a clearer view of the areas that are lacking and also to ensure no overlap.**

B **Set goals clearly. Define the areas that are practical and achievable with technologies that are emerging in the years ahead. Factors to consider include the density and terrain of a city. These may enhance or limit the rollout of some technologies.**

C **Develop a long-term plan. As technology changes so quickly, and standards evolve with new players entering the market, the plan has to include enough flexibility for the inclusion of new advancements. Vendor lock-in has to be avoided.**

One lesson which NEC has learnt over the decades helping shape future cities is that technology adoption has to do with more than just the latest technology.

The future holds much promise when it comes to innovations that are starting to promise safer city living. Yet, much of this requires deeper consideration. How will individuals take to the new technology, for example? Are the ways we use to test user acceptance still valid today, given the different aspirations of citizens everywhere?

Ultimately, city leaders who best understand the public sentiment are in the best position to answer those questions. A decision to deploy a technology could open up opportunities and impact thousands and perhaps even millions of citizens.

NEC Public Safety

At NEC, we have the solutions to help create a better, safer city. We have decades of experience working with governments, city planners and other public agencies in projects as varied as identification to public transport. Our solutions include national identification, law enforcement, immigration, protection of critical installations, safeguarding of cyber infrastructure and emergency and disaster response.

While bringing together the latest cutting-edge technology, NEC's team also possesses the experience and expertise to deal with projects – both private and government – on municipal and international levels.

Indeed, many of the technologies required to build a safer city are created from NEC's R&D facilities in Japan, Britain, China, Germany, Singapore and the US. Internationally, they have been proven as well. NEC is the most accurate for both fingerprint recognition and still-face recognition, according to tests run by the National Institute of Standards and Technology (NIST) in the US.

What's also unique about NEC is our expertise in both infrastructure and identity management. We have been working on natural or non-human infrastructure issues, as well as identifying incidents triggered by individuals, to better develop a secure and safe city.

In terms of protecting critical infrastructure, NEC has solutions to enhance the security in sensitive installations such as a city's water supply, power grid and telecommunications network. For example, NEC has high sensitivity cameras to capture video images, even in low light. NEC's behaviour detection systems can analyse the data and automatically detect suspicious behaviour.

As for incidents triggered by individuals, we are experienced in the areas of enforcement and identity resolution.

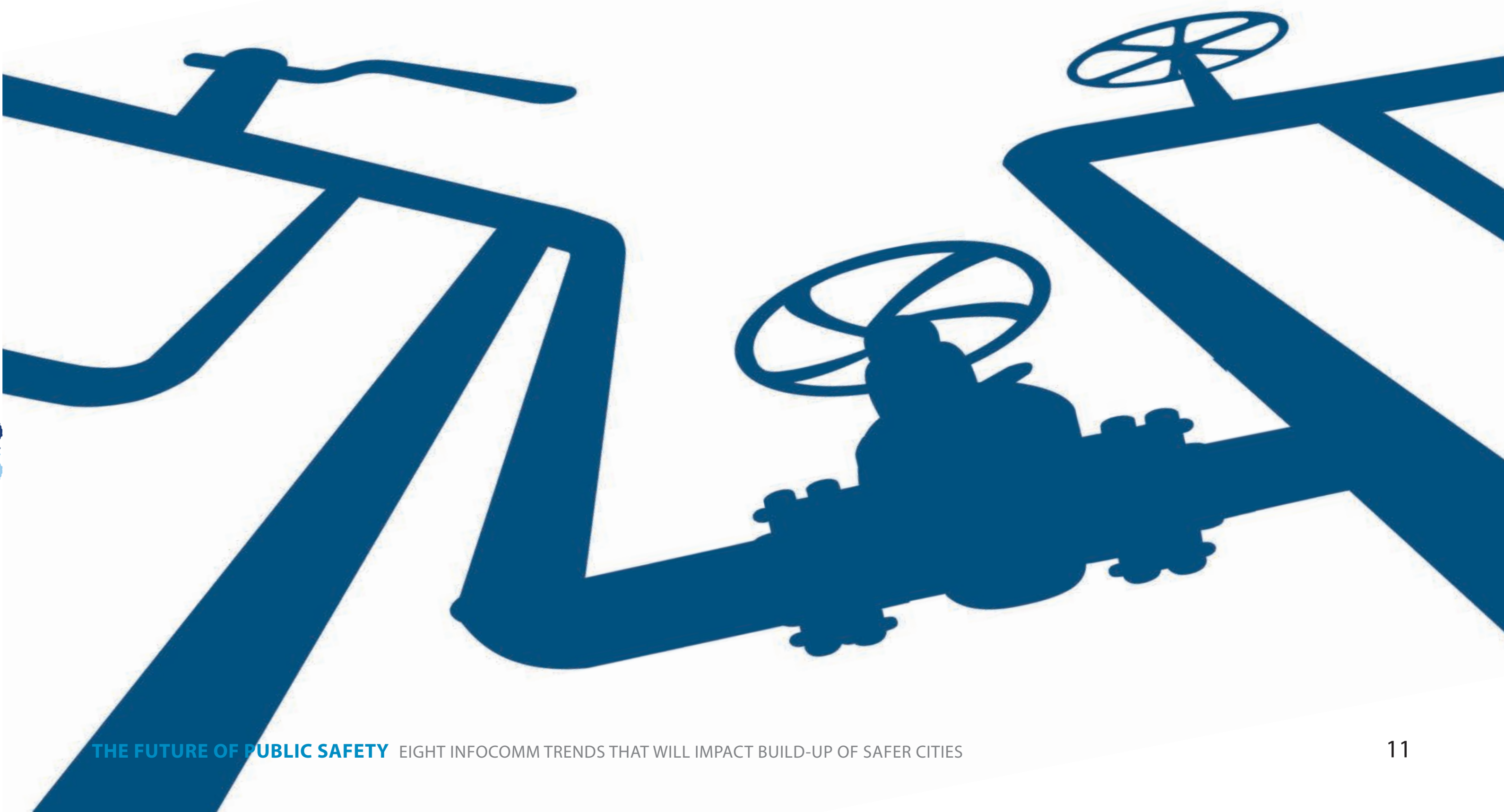
To-date, there are some 500 customers in more than 30 countries around the world who are using NEC's biometrics solutions. They have allowed countries to safeguard their border checkpoints, airports, seaports and other entry points.

Most importantly, our success stories around the world speak for themselves.

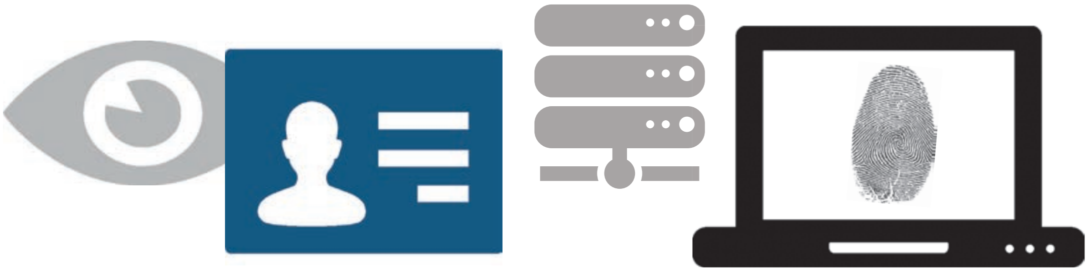
Singapore: In December 2012, NEC signed a three-year-agreement with Interpol to develop core elements of the Digital Crime Centre established at the Interpol Global Complex in Singapore. NEC will provide technical and human resources to establish a Digital Forensic and Cyber-Fusion Centre at Interpol's complex.

The Digital Forensic Lab will focus on identifying and test-bedding digital forensic technology and methodologies to help investigators better coordinate and conduct digital crime investigations. The Cyber-Fusion Centre will provide a platform for law enforcement to collaborate with the Internet security industry to effectively combat digital crime.

Working with NEC, Singapore was also one of the first countries to issue biometric passports in 2006. NEC developed the e-passports that allow Singapore citizens to clear immigration via an enhanced immigration automated clearance system using their normal passports as well as their biometric passports. Most people are able to clear immigration via the automated lane, thus freeing up officers to focus on other tasks.



Continued from page 12



Bolivia: In just 75 days, NEC helped to create an electoral voter roll for Bolivia using biometric data that enfranchised Bolivians and enabled them to vote in the presidential elections of 2009. Working with the National Electoral Court of Bolivia, NEC managed to create an electoral roll registering the voters living in Bolivia and abroad that was both accurate and reliable.

The solution consisted of NEC's AFIS (automated fingerprint identification system) and facial recognition technology, hardware, software, and staff training and support. As a result of their efforts, Bolivians living overseas were able to vote for the first time, and the voter list swelled from 3.5 to 5.2 million voters, allowing truly democratic elections for the first time in many years. Duplicate voters were also purged from the list.

South Africa: In 2001, NEC worked with South Africa to create a digital database of existing and new fingerprints that could be processed, verified and authenticated in real time. The Home Affairs National Identification System leveraged on NEC's AFIS to handle more than 30 million digital records.

Today, the system can handle as many as 70,000 searches in a single day. With the new system replacing a previous paper-based system, citizens can easily access public services and transactions. Queues are shorter, delays have been reduced, and the accuracy of the system has dramatically reduced the possibility of fraud and identity theft.

United States: In 2013, NEC will be modernising the multi-state criminal identification system run by the Western Identification Network (WIN) in the United States, which provides identification services to the law enforcement agencies and citizens of its member states. Together, the states of Alaska, Idaho, Montana, Nevada, Oregon, Utah, Washington, Wyoming, and California (as an interface member), have a database of about 28 million fingerprint records.

The updated system will include advanced identification capabilities such as high-resolution palm and fingerprint matching and other emerging biometric functions, disaster recovery facilities, and enhanced system performance. It will also incorporate key elements of NEC's cloud-based offerings – such as FBI-compliant data centres, Network Operations Centre, remote-managed services, and server virtualisation – that will be used to increase system security, reliability, and maintainability.

We believe our solutions can make cities safer and better.

To find out how they can benefit your city, contact us at safety@gsd.jp.nec.com

References

1. The Systems of Systems Approach for Interoperable Communications http://www.safecomprogram.gov/library/Lists/Library/Attachments/144/SOSApproachforInteroperableCommunications_02.pdf

2. US Intelligent Transportation Systems, Joint Program Office http://www.its.dot.gov/NG911/

3. Public Safety through ICT http://www.nec.com/en/global/solutions/safety/pdf/security.pdf

4. Beware the Big Errors of Big Data http://www.wired.com/opinion/2013/02/big-data-means-big-errors-people/

5. Internet of Things (IoT) & Machine-To-Machine (M2M) Communication Market – Advanced Technologies, Future Cities & Adoption Trends, Roadmaps & Worldwide Forecasts (2012 – 2017) http://www.marketsandmarkets.com/Market-Reports/internet-of-things-market-573.html

6. Internet of Things Poses Big Questions http://online.wsj.com/article/SB10001424127887323899704578583372300514886.html

7. Gartner Says Worldwide PC, Tablet and Mobile Phone Combined Shipments to Reach 2.4 Billion Units in 2013 http://www.gartner.com/newsroom/id/2408515

8. The promise of software defined networking http://www.networkworld.com/news/2013/070113-sdn-271298.html

9. Software-Defined Networking Market Expected to Reach $35 Billion by 2018 http://www.sdncentral.com/sdn-blog/sdn-market-sizing/2013/04/

10. Smart Grid Sensor Market Set to Double in Size by 2014 http://www.imsresearch.com/press-release/smart_grid_sensor_market_set_to_double_in_size_by_2014

Contributors

- Paul Wang (PhD), Chief Technology Officer, Global Safety Division, NEC Corporation.
- Kris Ranganath, Director of Technology & Solutions, Biometrics Solutions Division, NEC Corporation of America.
- Douglas Tang, Senior Director & Global Lead of Cyber Security, Global Safety Division, NEC Corporation.

This paper is published by NEC Global Safety Division. Some of the ideas in the paper are aspirational, and NEC is working towards realising these ideas in our vision of making cities safer.

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: No.1 Maritime Square #12-10, HarbourFront Centre, Singapore 099253
For enquiries, please contact safety@gsd.jp.nec.com

nec.com/safety

WE MAKE CITIES SAFER
Using technologies to safeguard lives and property

Citizen Services & Immigration Control
Law Enforcement
Critical Infrastructure Management
Public Administration Services
Information Management
Emergency & Disaster Management
Inter-Agency Collaboration

The information contained in this white paper is the proprietary and exclusive asset of NEC unless otherwise indicated. No part of this white paper, in whole or in part, may be reproduced, stored or transmitted without the prior written permission of NEC. Unauthorised use or disclosure may be considered unlawful. It is intended for information purposes only, and may not be incorporated into any binding contract. This white paper is current at the date of writing only and NEC will not be responsible for updating the reader of any future changes in in circumstance which may affect the accuracy of the information contained in this white paper.