WHITEPAPER

Orchestrating a brighter world NEC

SAFER CITIES SMARTER LIVES

Creating safer, more secure urban
societies through technology

CONTENTS

Making an Impact on Everyday Life

In the midst of what is termed the Fourth Industrial Revolution, the world has seen unprecedented advances that have come together to impact everyday life like never before. The convergence of cloud computing, artificial intelligence, the Internet of Things and many related innovations in the past five years has brought about profound change and disruption to countries, industries and the people who are part of them.

In many ways, the future looks bright. Autonomous cars promise more efficient, safer travel on the roads. A connected city gives citizens up-to-date information of changes in train schedules, allows them to check in at an airport without fuss and enjoy many e-services that they increasingly depend on.

Yet, safety and security are still at the heart of everyday life in urban societies. At a time when city living is promising to be safer, more pleasant, things could change in an instant with the spectre of terrorist attacks. Meshed in with this are the increasing scourge of cyber threats, which target anything from critical infrastructure such as dams to personal computers.

The senseless bomb attack in a concert in Manchester in May 2017 killed scores of innocent victims, some of them children. Just weeks before that, an unrelated malware had spread globally on vulnerable computers and locked out users at home, in offices and even at hospitals. They are reminders that the world continues to face severe threats.

Since the terrible tragedy of September 11, 2001, the concept of safety has never been far from the priorities of city life. Technologies have to work together to empower city planners, so they can protect citizens and enhance their quality of life.

The good news is they have made a clear impact. Advanced face recognition, for example, is making it possible to track persons of interest across various locations, even if the camera footage is of low quality and not ideal. Increasingly, artificial intelligence will make a difference in helping human operators identify threats in both the cyber and physical worlds, fusing the raw data collected to make sense of a situation swiftly for decision makers.

For an idea of how a smart and safer city has evolved, one only has to look to Singapore. Its smart nation efforts have involved the use of smart surveillance technologies to detect suspicious behaviour at sensitive locations such as train stations, for example. Using a mobile app, its citizens can actively report a security incident by uploading videos or images easily.

This is not just about the technology. If the past five years have been about finding the right digital tools to do the job, the key today is also making sure they bring demonstrable impact to citizens. Many of them may not “see” these technologies at work, but they will understand that a safer city is one that is constantly keeping threats at bay.

In the following chapters, we aim to show the evolution of this approach over the years. They are a culmination of our years of experience working with cities around the globe to improve the quality of urban living. We believe they will provide a way forward to achieving that goal.

Tan Boon Chin
Managing Director,
NEC Global Safety Division

CHAPTER 1

Evolving Urban Societies

Going from connecting the dots to acting on the new knowledge available, smart cities will also have to become safer cities for citizens in the physical and cyber worlds.

Speak about a smart city just a few years ago and much of the conversation would have stayed on future technologies that could one day uplift the quality of life for citizens. Much depended on the maturing of these innovations.

Today, the "what ifs" have been turned into certainties. Smart city innovations have sprouted around the world as planners put in place bold initiatives to connect citizens to digital services that make the urban environment more liveable.

From making a city safer through urban surveillance to enabling faster airport transits by utilising facial recognition, new digital solutions are already making a big difference every day. Much of the change has come about through the decisive action of city planners and the pace of technological development.

Cloud computing has given access to unlimited resources, enabling companies from startups to established enterprises to build new digital services and apps at a scale that they could only dream of in the past.

The Internet of Things (IoT) is coming alive all around, from smart homes that bring automation via a smartphone app, to connected cars that self-drive themselves without human intervention. Sensors are truly coming online, after years of being talked about as the next big thing.

What this brings is the next phase. As more data is recorded, it has to provide the accurate insights needed by decision makers to plan and act – often in real time. Data analytics is an area that is growing fast, helped now by artificial intelligence (AI) and machine learning, which both help make sense of the fast-flowing flood of data and turn it into actionable information.

Cities are not waiting for the next innovation to spring up, even as smart and safer city technologies are evolving all the time. Early adopters have already reaped the benefits of being at the forefront of what some have called the Fourth Industrial Revolution.

After the steam engine, electricity and the PC, the digital technology that is behind much of the smart city innovation today is already making a mark in many places.

In Singapore, the government push to turn the city-state into a smart nation has showcased the potential and impact of such innovations. A local taxi hailing app company is using its smarts to provide a private bus service to pick up passengers at crowdsourced locations during peak hours, when a cab is hard to come by.

Meanwhile, a mobile app developed by the government, called MyResponder, has alerted volunteers nearby to come to the aid of persons suffering from a heart attack. In the crucial moments before an ambulance arrives, it has helped save lives.

The phenomenon is worldwide. In Colombia, a facial recognition system installed in a popular football stadium has enabled the authorities to have better crowd control. Known trouble makers and gang members who have been put on a ban list are automatically stopped from entering. Keeping them out means football fans, including children, can enjoy their matches without the spectre of violence.

NEW OPPORTUNITIES AS CHALLENGES ARISE

Yet, the smart city transformation is only just beginning. Already, there are new challenges that cities face, as more people migrate to urban areas in search of better jobs and an opportunity for a better life. Over-crowdedness will put a strain on public infrastructure while poverty in urban areas will breed crime if social inequalities are not addressed.

In 1990, 43 per cent of the world's population lived in urban areas, according to the United Nations (UN). By 2015, this had risen to 54 per cent. While some cities have well planned housing, others have failed to provide adequately for citizens. In 2010, as many as 980 million urban households lacked decent housing, as will another 600 million by 2030[1].

Arising from this are growing insecurity and urban risk. Crime and violence have become threats to the well-being of citizens in many urban environments, as a result. At the same time, terrorism is a scourge that has expanded around the world.

From 2000 to 2014, the number of people killed by terrorist attacks rose nine-fold. In 2014 alone, the number of deaths rose by 80 per cent – the largest annual increase in 15 years, according to the UN.

There is another growing threat of late. As users and cities become connected, so too are an increasingly sophisticated cyber criminal network keen to exploit vulnerabilities in new systems. Ransomware alone cost victims US$1 billion in 2016[2].

From state-sponsored hackers that attack critical infrastructure like power grids to sophisticated criminals who trade credit card numbers on the DarkNet, cyber criminals have become more sophisticated and organised. They pose a serious threat to smart cities that do not have the capability to defend themselves.

Indeed, any smart city in future would have to be a safe city. Cyber criminals who have the ability to steal medical records and hold a hospital ransom would compromise the trust that citizens have in a smart health service. In the same way, city planners would have to prepare for a day when these attackers will penetrate the best defences, given how many new vulnerabilities are found each day in interconnected software and systems.

A SMART CITY MUST BE A SAFE CITY

As cyber threats become more serious, there has already been a shift towards more a robust cyber security posture in many countries that seek to become connected.

Even as they install more sensors, set up IoT networks and collect data across a wide spectrum of sources, the challenge is now to secure that precious data and ensure that digital services are resilient to new threats. How can city planners provide a safer environment in both the physical and digital worlds?

This could involve moving up the development ladder to be a safer city. At the basic level, a city will start setting up intelligent sensors to discover the physical and online worlds. While sensors ranging from cameras to cyber security sensors are becoming cheaper and easier to install and connect, this is usually just the beginning of the journey for an evolving smart city.

What they would next have to do is to build a security environment that monitors the network and traffic linked to these sensors. This could be carried out at a cyber security operations centre that can detect possible intrusions into a network or a physical location.

The next step up would be to integrate all the data available and analyse it for possible breaches, whether this is pointing to a physical or cyber scenario. A potential terrorist targeting a government office may have scoped out its website and also physically surveyed weak points at its location.

Smart surveillance systems will be able to detect the suspect as he physically nears the building. Matching him to a database of known threat actors with a real-time facial recognition system, the authorities can be alerted in time to an impending attack. Using a network of cameras, they can track him across multiple locations. They can use his digital trail, such as credit card payments or ATM withdrawals, to keep a lookout for him even if he is out of visual range.

AI will play a crucial role in this, in bringing cities to the next level. Unlike before, when a human operator has to manually make sense of all the data coming onto his dashboard, the analysis from AI will enable decision makers to better understand a situation. It does so by learning from the data it is fed and assessing the risks that are faced at that moment.

This would lead to an important step up – a calibrated response. With information dissemination, situation awareness and risk assessment all carried out in real time, multiple government agencies from homeland security to emergency rescue can spring into action to address a threat. Key to this is the automated processes that are involved, to enable an immediate, coordinated response that could make all the difference in an emergency.

As smart cities grow in the years ahead, such an integrated approach will prove crucial to a sustainable urban environment that is both well networked and secure.

Indeed, as citizens become more reliant on the growing number of digital services for everyday living, the need to integrate what are still separate environments today will be imperative to a successful smart city. If being smart has been about connecting the dots so far, the next step is the ability to create deep, meaningful impact with that new knowledge.

[1] http://wcr.unhabitat.org/wp-content/uploads/2017/02/WCR-2016_-Abridged-version-1.pdf
[2] http://www.zdnet.com/article/the-cost-of-ransomware-attacks-1-billion-this-year/

CHAPTER 2

Future of Public Safety

Seven infocomm trends that are impacting the build-up of safer cities

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.

"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? "

Increasingly, in inter-connected cities, infocomm technologies empower new nerve centres that are necessary to keep things ticking, solve complex problems and make life better for the average citizen. They enable safer, more sustainable living and working spaces.

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.

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.

With the right innovation tools, city planners can build capacity and translate all the information coming through their feeds into action. Here are seven technology trends and issues that are now shaping such efforts.

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 Boston bomber in 2013, they will have had to look through thousands of images to find a person of interest.

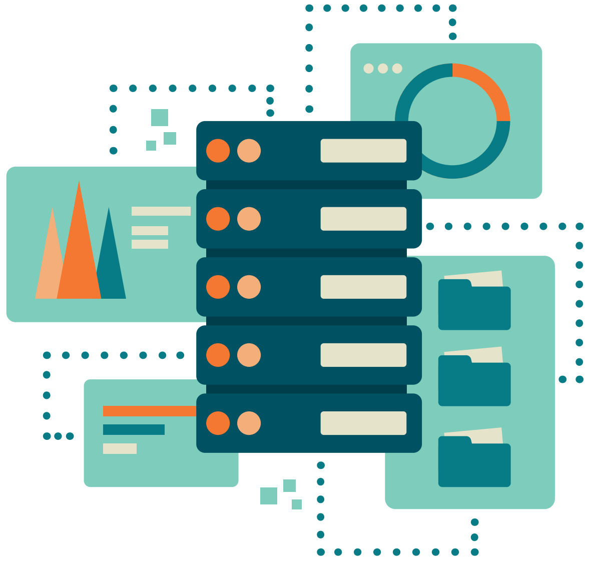
What can assist here are smart sensors that not only provide plain video but also GPS location information, for example. Better still, if a video analytics system can recognise facial patterns and zoom in to look for a particular facial feature on a suspect. This has to be both accurate and fast.

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.

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.

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.

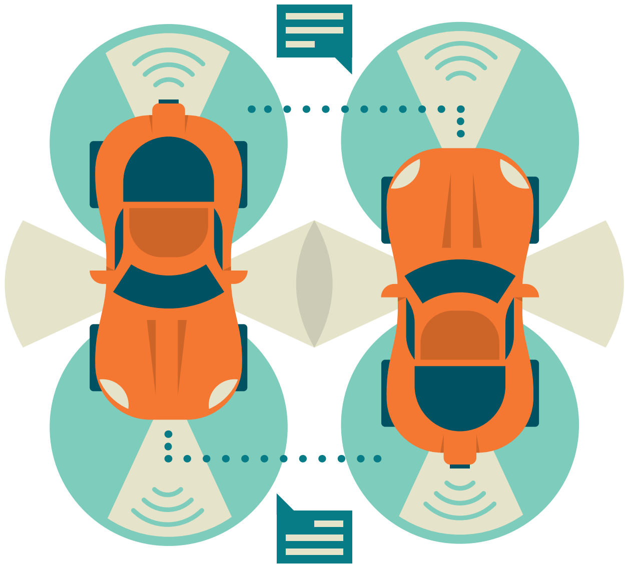
One simple question to ask is whether a Big Data solution provider uses relevant data sets and big-enough sample sizes. Traditionally, statisticians follow these rules, and so should any data that is input into a system to find new trends and predictions.

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. SMART NETWORKS



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 decisionmakers.

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.

Communications among smart devices 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.

Solutions to guarantee authentication but also non-repudiation and privacy protection for vehicle-to-vehicle communications are being finalised mostly in Europe and US.

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 new devices that provide 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 body cameras that stream a real-time video feed to a nearby mobile station, which can then inform them over a wireless link what to look out for.

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 is not just in the technology. Users have to be able to get used to the technology. Wearing a body camera 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. IOT NETWORKS

With so many non-human sensors, meters and even connected wearable devices "talking" to one another, the IoT network is one that has to be built to 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.

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.

Increasingly, 5G is being touted as the future. With speeds topping 1Gbps and latency as low as 1 millisecond, it is seen by many as the ideal connection for future IoT devices. A person may even remotely "drive" a vehicle or operate an excavator with the near-instantaneous reaction time.

Other wireless technologies such as NB-IoT (narrow-band IoT) are already being rolled out around the world. Specifically catering to linking up low-latency, low-bandwidth devices, they enable cities to be connected without jostling for a lane on the cellular networks that are often congested by human users.

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. DRIVERLESS CARS

Car owners may at be at the wheel in the future, but many will not have to place their hands on the steering wheel or even stepping on the brakes. Autonomous vehicles, now possible thanks to the advancement of AI, will one day be as common as vehicles driven by humans. That one day, according to car makers from Tesla to Volvo, could be less than 10 years.

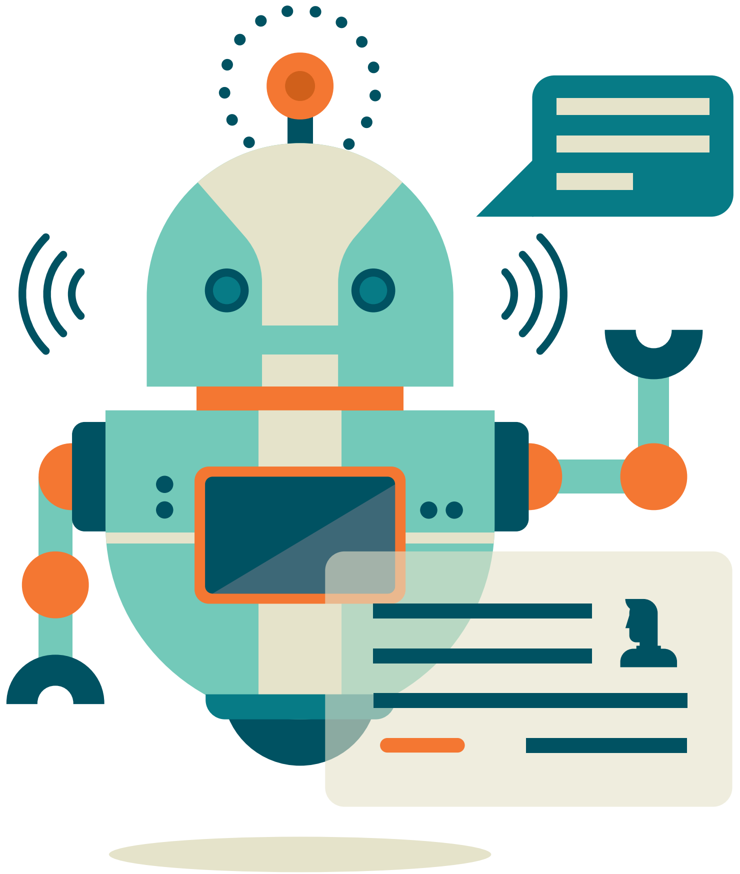
Already, many trials have been carried out for autonomous vehicles, from buses to taxis, around the world. In December 2016, the first self-driving Uber cars started operating in San Francisco. These Volvo XC90 vehicles came with all the sensors needed onboard and there was still a safety driver inside the vehicle to take over when needed.

However, fully autonomous vehicles will be a few years away, at least. The main reason is safety. In 2016, a man driving a Tesla car was killed in an accident after ignoring warnings to take over from the autonomous system. Since then, autonomous car makers have doubled down on their efforts to make these vehicles even safer.

In a city of the future, autonomous cars have clear benefits. Unlike humans who may be tired after a day of work and lose concentration, AI does not. At the same time, it can automatically find the fastest, safest routes to a destination. This helps to reduce city-wide congestion.

In fast-expanding cities struggling to cope with transporting millions of commuters each day, autonomous vehicles will make a difference by increasing the availability of public transport. Bus drivers may have to be rotated on shifts, but AI does not tire. This enables them to continue running a public transport service efficiently – once the kinks with autonomous vehicles are ironed out in the years ahead.

7. ROBOTICS



In the 1980s, robots came to the fore for their efficiency on the manufacturing floor. Today's robots are not only used to make goods more efficiently, they can serve a wider variety of roles.

For example, they can be used in cities where there is labour shortage. Instead of having waiters attend to every customer need at a restaurant, robots may be able to do the simple tasks. These include collecting the used cutlery and cleaning a table after a customer has finished his meal.

Robots can play more interactive roles as well. Socially intelligent robots may be placed to help people at airport information counters, to direct them to the right locations. They may usher travellers to the right queue at an airport immigration counter, freeing up humans to take on more
challenging tasks.

Much of the intelligence could be in the form of software as well. Chatbots, now used in many websites, enable service providers to easily answer commonly asked questions. They are already being deployed by town councils in Britain, as intelligent personal assistants, to apply logic and help resolve problems for residents.

In the future, these chatbots could possibly perform transactions as well. This means they can answer personalised questions, for example, by helping a person apply for a permit or license with a government agency. As the software matures, there is no limiting the physical tasks that a robot that carry out as well.

In a library of the future, a robot could be the all-knowing librarian that can not only answer tough questions, but go fetch the book that you are looking for. Robotics have come a long way over the decades and it is poised by the big leap in the coming years, thanks to the recent advancements in AI and data analytics.

TOWARDS SAFER CITIES

In building safer, more liveable cities, planners will have to identify which of the key trends and issues are topmost on their agenda. 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.

CHAPTER 3

Smart City Lessons from Singapore

Collecting and analysing data from an array of sensors and cameras, Singapore rolled out a futuristic Test Bed for a safer city in 2013. Here are some learning points from one of the first such deployments.

When Singapore's government planners first considered high-tech plans in 2012 to make the city-state safer and more secure, they were in a situation that many foreign counterparts could only envy.

Well-connected, efficient and highly urbanised, the country of 5.4 million people was as ready as any to embrace the timely information that an array of on-the-ground sensors and cameras could immediately feed decision makers. The widespread use of social media also meant that users were tuned in to the latest news, sometimes becoming active participants or witnesses to developing incidents.

With a safe city system, police forces could react swiftly to a crowd that displayed unruly behaviour. Emergency services could detect potentially unsafe locations where an increased number of people may make an evacuation difficult. Floods would be more easily detected with live monitoring of water levels.

Yet, despite Singapore's renowned advancements, it faced a number of challenges not unlike many other cities. One key concern was optimising the limited manpower available, while maintaining effective day-to-day city management activities such as ensuring smooth vehicular traffic, upholding law and order and managing emergencies.

With a fast-paced economy came an expectation for fast, efficient service as well. Should the public be first on the scene of an incident, for example, emergency responders were expected to be on the ground within a short period of time, rendering assistance or upholding public order.

A COMPREHENSIVE PROJECT

With these factors in mind, the Singapore government looked far into the future for a comprehensive safe city project in 2012. The country's planners had often been known to be far-sighted, ready to adopt new ways of doing things. In developing a safer city, they were no different. They expected the project to run in multiple phases in three to four years, eventually leading to ready-to-market solutions.

In January 2013, the Singapore government issued a Safe City Test Bed Call for Collaboration that would kick start a year-long pilot project. It would involve the specially set-up Safety & Security Industry Programme Office (SSIPO), as well as a number of participating agencies, including police, civil defence, environment and water, land transport and homeland security, to develop a comprehensive system to address a wide spectrum of safety and security concerns.

Collecting and analysing data from an array of sensors and cameras, Singapore rolled out a futuristic Test Bed for a safer city.

The goals were clear. Police forces should be able to have better situational awareness that enabled them to better react to fast-developing incidents. With timely on-the-ground information, emergency services could better facilitate evacuation, for example, at a popular event where a fire may have broken out.

At the command level, a team coordinating to any home front crisis incident should have better global awareness, which would allow for improved decision making.

Singapore already had existing camera systems and various sensors providing data feeds back to government agencies. A new system making use of new sensor technologies and analytics on the fly would do more, by enabling decision makers to better comprehend a situation and make critical and timely decisions.

Key to this would be pulling all the data together in a way that made the information meaningful. In a crisis, decision makers had to see the big picture, literally, on a large screen to make sense of what was being fed from cameras and sensors.

The SSIPO identified four sites to test the technologies. In one of them, a consortium led by NEC Asia Pacific won a bid in May 2013 to develop a safe city Test Bed for the Ministry of Home Affairs and the Economic Development Board (EDB).

With its experience developing safe city solutions, NEC would bring technology proven in markets around the world to Singapore.

A SOPHISTICATED TEST BED

Earlier, in the Argentinean city of Tigre, NEC had set up an urban surveillance proof-of-concept project to enable city authorities to better monitor activities at strategic locations.

In Singapore, the NEC team knew that it was preparing for an exciting Test Bed. Though similar in spirit, the SSIPO project would come with greater complexity and sophistication, something which the NEC team was well prepared for.

The police would want to be able to detect aggression or fighting easily, so that officers on patrol nearby can be alerted more swiftly.

Singapore agencies also wanted awareness of the traffic situation, through camera surveillance, and be able to better react to a traffic accident or the occasional congestion.

At the same time, the environment authorities concerned with the cleanliness of city streets wanted a way to detect if someone was littering.

Also useful to them would be a surveillance system that indicated how clean a place was, so cleaners could be deployed more efficiently. For the nation's security services, the safe city system from NEC had to pick up suspicious persons loitering at train stations.

Perhaps more importantly, the sensors and cameras had to provide information in a holistic way to help officers manage incidents. Armed with actionable intelligence, commanders could then better support officers on the ground with improved assessments of knock-on effects from an incident.

The system that NEC was building had to provide predictive analysis, to quickly explain how a situation would develop. Traffic flow, for example, would be severely hampered if there was a power outage in an area, and government agencies needed that insight.

USING THE RIGHT TECHNOLOGIES

This called for a number of technologies, which NEC pulled together with consortium members Esri Singapore, Force 21, G Element, Greenfossil, iOmniscient, Oracle and ZWEEC Analytics, as building blocks for a seamless safe city solution.

It would use a number of sensors – physical ones for acoustic, video and smell as well as online ones for social media reactions – to identify an incident of interest. In particular, a hemispheric camera (HemCam) would be able to capture images without the distortion usually associated with wide-angle fisheye lenses.

An IoT network would have to be built to allow these sensors to communicate and ultimately connect back to a central system for live feeds of what was happening on the ground. Sensors would be dynamically added or dropped.

Separately, an appliance would have to be installed to provide various agencies with the information they required. This inter-agency information appliance would, however, authenticate and track the authorised accounts that access the data. Users would only receive information on a need-to-know basis.

In addition, a system that made use of semantic web-based risk models would attempt to make sense of cyber information. It would monitor postings based on predefined risk models and identify if a situation required the attention of various agencies.

Finally, the NEC-led team also had to develop a geo-spatial visualisation platform that would put all the data in context. On a large screen, this fusion of information would have to make instant sense to operators at a command centre.

UPGRADED CAPABILITIES

The results from the Test Beds were clear soon after the first deployments went online in late 2013, when the sensors on the ground started sending information to the relevant agencies.

In urban surveillance, the potential of early incident detection became clear. Video analytics could help detect a snatch thief thronging through a busy weekend crowd. Similarly, a fight occurring in view of cameras would be easily picked up.

Video analytics would detect the particular motions as symptomatic of a fight, along with aggressive action. Audio analysis then enabled the system to understand that someone was shouting or crying, whether in anger or distress.

This provided vital information to officers reacting to a situation. But that was not all. The system would automatically look for potential points of congestion or blockage in the area, where the traffic flow might be affected.

It would be able to alert relevant agencies and provide a visual map layout of the ground situation to both ambulance and security services. As they headed to the scene, they could be fed live information on the best route in and out of the area.

All in, the fusion of the various technologies gave an unprecedented amount of actionable intelligence and improved command and control. With this, officers and commanders did not end up overwhelmed with information. Instead, with the raw feeds analysed and presented in a way that truly empowered them, their capabilities were upgraded to handle difficult situations.

The same technologies were used in other scenarios. Facial recognition and video analytics enabled officers to detect behaviour such as loitering. If an officer alerted to this found it necessary, he could then check for similar, repeated occurrences. If a group of people were known to be lurking around a sensitive location, for a potential crime, they could be flagged by the system.

Besides suspicious persons, advanced video analytics could also detect suspicious objects being abandoned. For example, if a person left behind a suitcase in a train station, the system could look up a list of persons associated with it by analysing previous video recordings.

Using a blend of facial recognition and clothes recognition, it would then display the last seen location of the persons of interest, as captured on video footage.

Apart from the country's security services, the Singapore Test Bed also benefited other agencies immensely. The same technology used to detect an abandoned object could be used to monitor if an object was missing.

For example, the authorities could check if someone had stolen items such as rubbish bins.

Agencies also benefited from a system that could detect crowds in a specified area. More crowds usually meant there was more rubbish to be cleared. Once the threshold for a "geo-fenced" area was reached, an alert could be triggered to an officer, who would determine if a cleaning crew had to be dispatched.

At the same time, a slightly different system helped the transport authorities monitor cars on the roads, to see if congestion was building up. This was done with traffic volume monitoring as well as surveillance of the travelling speed of cars through important stretches of roads.

This was especially helpful because the system also took in information from real-time traffic reports already available. Together, the fusion of information provided situation awareness via a geographic information service (GIS).

Yet another agency that would benefit from the safe city project was Singapore's water agency. With advanced video analytics, it could detect if water level had risen beyond a pre-defined level at many drains around the island. Once a certain level was reached, an alarm could be sent out to an officer, who would determine if a flood was imminent and send out appropriate alerts to people near to an affected area.

All in, 20 analytics capabilities were successfully tested. Some 370,000 faces were detected a day. Crowd behaviour was correctly detected 75 per cent of the time and crowd counting was 80 to 90 per cent accurate.

UNDERSTANDING THE INFORMATION

All that data, of course, would mean nothing if officers in charge were not able to make use of it in a timely fashion. This is where NEC's team made a difference. It had analytics to make sense of the data and sophisticated governance to guard its access.

At the most basic level, remote sensor analytics picked up primary data such as fight detection, abandoned object detection and crowd detection. Using NEC's MAG1C Bus system, this could also support analytics engines from other partners.

NEC's MAG1C Sense semantic analysis helped make sense of the data even further, by adding users' domain knowledge to the mix. Using ontology-based risk models, it analysed patterns and inferences to predict potential incidents and likely follow-on effects.

In turn, that intelligence was presented on a city map or 3D building model that incorporated trends, real-time events, content and spatial analysis. These visual tools, based on Esri's ArcGIS and G Element's Nucleus, enabled swift and effective decision making.

Finally, NEC's Information Governance Suite (IGS) enabled various agencies to access information they required, while protecting it using access rights. This meant various agencies collaborating on a situation could have access to a set of data – on a "need to know" basis.

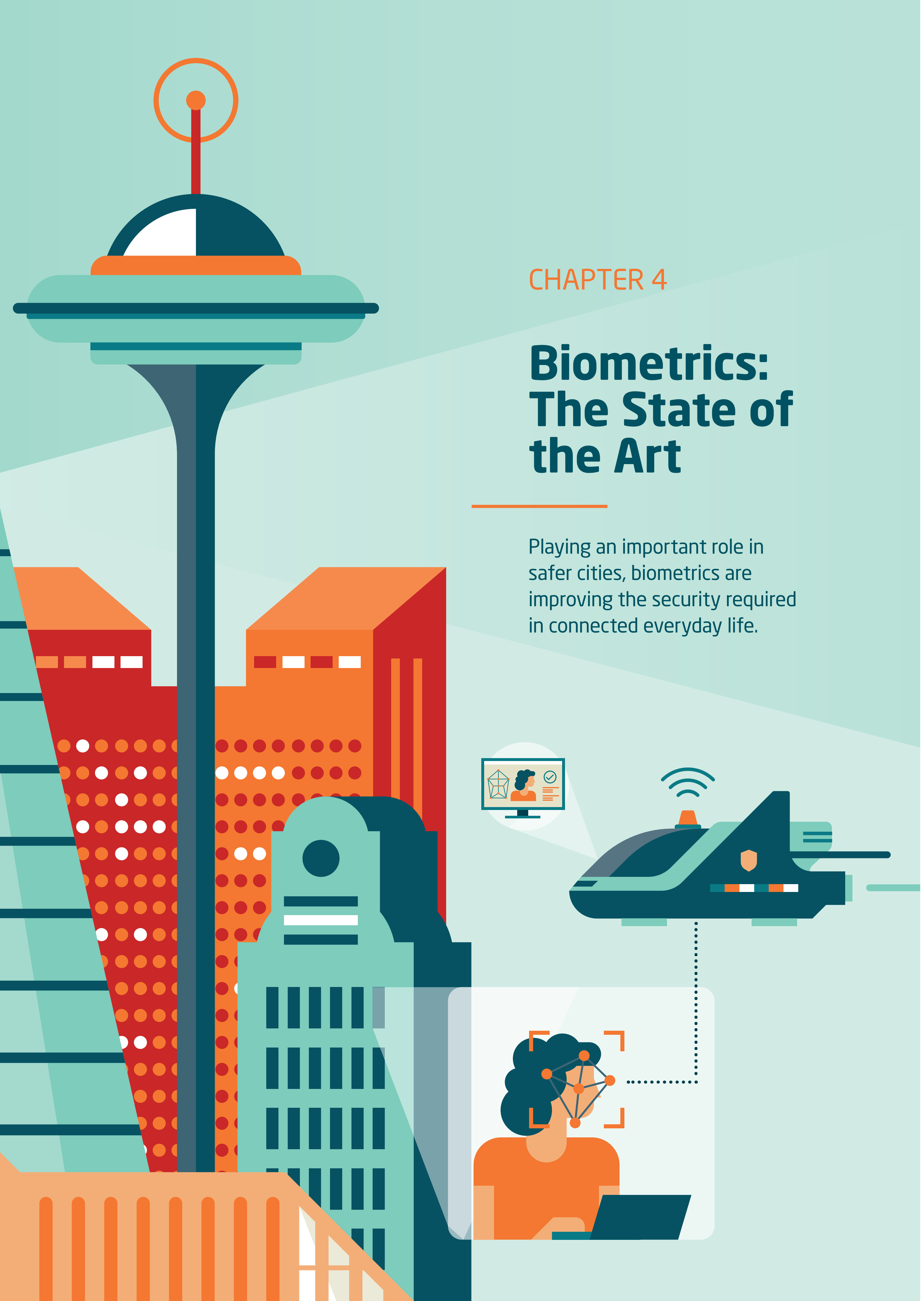
A COMMITTED PARTNER

Many lessons were learnt from the Singapore Test Bed. One was the importance of having all relevant agencies onboard a platform that would benefit from as much information as possible. At the same time, the trials also validated that a safe city solution would help address many of the challenges facing Singapore.

Perhaps most important in a project like Singapore's was the readiness and experience of technology vendors to meet the requirements of government agencies involved in the crucial job of ensuring safety and security in a city.

Throughout the Test Bed project, NEC spared no effort in refining small details in the system. It also ensured that it would work well with existing systems that were in place previously.

With decades of working with governments the world over, NEC was well-positioned in this area. Backed by cutting-edge innovations such as advanced biometrics and inter-agency collaboration tools, the company integrated the technologies of its consortium members to deliver a Test Bed that showed how a future city could keep safe and secure with the latest advancements.



CHAPTER 4

Biometrics: The State of the Art

Playing an important role in safer cities, biometrics are improving the security required in connected everyday life.

Biometric technologies use biological features such as fingerprints, veins, faces and irises to identify individuals. They greatly improve the accuracy and reliability of identification and verification systems by taking out the element of human error.

In the area of public safety, biometric technologies in the form of fingerprinting, iris and facial recognition have made a significant contribution to border control and law enforcement.

Biometrics has also played an important role in ensuring personal security, both in terms of facilitating the provision of social services at the national level as well as protecting personal devices and accounts from crackers.

Now, the rise of multi-modal biometrics provides new ways to improve public safety, user experience and protect personal privacy. The combination of multiple biometric parameters makes the technology much more robust against challenges.

Mobile biometrics and biometrics on the move are two other developments to look out for. The integration of biometrics technologies with mobile devices will reduce infrastructure costs, while the ease and convenience of non-invasive capture enabled by stand-off biometrics will spur its widespread adoption.

FROM BASIC TO ADVANCED TECHNOLOGY

Whether it be a student's distinctive facial feature recognised by a teacher taking the class' attendance, your signature on a check which allows money to be withdrawn from your bank account or your profile picture on Facebook which helps your friends find you; "basic" biometrics are firmly a part of everyday life.

Despite our heavy reliance on them, our current methods of identification and authentication are far from ideal. A study of Australian passport officers published in the journal PLOS ONE showed that the officers missed one out of every seven fake passport photos, and that trained staff were no more accurate than student volunteers.

This high error rate of 14 per cent is particularly worrying in the context of modern day air travel, where hundreds of thousands of people pass through airports each day. It is perhaps not altogether surprising then, that two out of the 227 people on-board the missing flight MH370 from 2014 were traveling on false identities[3].

The main weakness of basic biometrics is the high rate of human error. A new haircut can dramatically alter the way a person looks and signatures can be forged, for example. Non-biometric technologies have sought to reduce this subjectivity by relying instead on passwords or physical tokens to establish identity.

However, as anyone who has forgotten their password or left their staff card at home knows, these methods can sometimes lead to frustrating situations. Rather than replace basic biometrics with non-biometric technologies, advanced biometrics make the identification of unique physiological or behavioural traits much more accurate and reliable.

After more than two decades of research, biometric technologies have matured and advanced to the point where they are able to achieve sophisticated functions and outperform human abilities.

[3] https://www.theguardian.com/world/2014/mar/11/passengers-malaysian-plane-mh370-iranian-forged-passports

In 2017, the U.S. National Institute of Standards and Technology (NIST) reported NEC's face recognition technology had an accuracy of 99.2 per cent when matching a person as he walked through an airport passenger gate.

Ultimately, what biometrics enables is automated access control and identity management; replacing human, error-prone processes with technology.

There are two main types of biometrics:

1. identification or recognition, or one-to-many, where the aim is to match a single individual to multiple entries in a biometric database

2. verification or authentication, also known as one-to-one, where the aim is to prove that the person is really who one claims to be.

PERSONAL SAFETY

Being able to verify identity is not only important for border control and law enforcement agencies, but could also help to prevent fraud, increase access to governmental services and even promote democratic participation.

Biometrics, where the person serves as a marker of identity rather than a document, could be particularly useful in developing countries where literacy rates are low. In 2009, the government of India embarked on a massive project to enrol its 1.2 billion residents into the biometrics-based Unique Identification Program, also known as Aadhaar.

Intended as a means to fight corruption particularly in the issuing of subsidies, an Aadhaar social security number also provides the holder with access to other services such as healthcare and education. It also serves as a voter registration system, thereby helping to prevent electoral roll fraud.

Although costs have been substantial, amounting to US$574 million as of September 2013 according to the Unique Identification Authority of India (UIDAI), benefits include fewer leakages, lower transaction costs and improved labour mobility.

In fact, a cost-benefit analysis by the National Institute of Public Finance and Policy (NIPFP) shows that the implementation of Aadhaar yields an internal rate of returns of 53 per cent, even though it only takes into account the savings by the government.

If intangible benefits and systemic benefits to the economy are also accounted for, the rate of return on investment in Aadhaar would be even higher.

While government agencies have been quick to adopt biometric technologies, the take-up rate has been slower among individuals, largely hampered by high costs. Nonetheless, there is evidence that user acceptance is growing as the cost of mature biometric technologies falls.

In fact, a number of existing biometrics users is already substantial, driven largely by the adoption of biometrics technologies in the consumer smartphone market.

Tech giant Apple first introduced their fingerprint locking system known as TouchID with the launch of the iPhone 5S in 2013, causing competitors Samsung to incorporate the same technology into the Galaxy Tab S. The iPhone 6 that came later took the technology further, integrating fingerprint scanning with near field communications (NFC) to enable mobile payments.

A market report by Frost and Sullivan predicts that there will be an explosive growth in the biometric smartphone market within the next few years, expanding more than ten times from 43 million in 2013 to 471 million in 2017[4].

As online shopping becomes more mainstream, there has been a greater demand for more robust authentication processes. Existing methods using numbers exposed on credit cards and password-token combinations are not foolproof. In 2015, consumers lost US$158 billion to cyber crime globally, according to a Symantec report[5].

Biometrics provides a much safer way to authenticate high value transactions. For example, it would allow continuous authentication, where the user's iris is tracked throughout the authentication process. A secondary but related need is the desire for greater convenience. Unlike passwords or tokens commonly used for two-factor authentication, personal physical features cannot be lost or stolen.

Biometric technology will do away with the hassle of carrying around multiple authentication devices and having to remember complex and non-intuitive passwords. Recognising the potential for retail applications, Chinese online payments powerhouse Alipay entered into a partnership with technology company Huawei to incorporate mobile payments into Huawei's flagship phone, the Mate 7, in 2014.

Aside from the cost factor, one of the considerations preventing the mass adoption of biometric technologies has been the issue of privacy. Although the fact that biometric features are irreplaceable makes them secure, it also means that steps must be taken that they do not fall into the wrong hands.

In particular, consumers are concerned that biometric information in the form of facial photographs and fingerprints are easily available, and therefore open to theft.

However, what many consumers may not realise is that biometric technologies such as fingerprint and facial scanners do not store an actual image of the fingerprint, iris or face, but instead digitally encode the information in what is known as a template.

Each device which captures biometric information would use different features to develop a template, making it difficult for a template captured on one device to be used to authenticate a device using a different template system. Furthermore, it is nearly impossible to reconstruct the original image based on the template data.

VIDEO ANALYTICS

As facial recognition technology continues to mature, the next key technology that looks set to grow in importance is video analytics. Traditionally, video surveillance has been used to secure restricted areas such as airport runways or hangars. This process is becoming increasingly automated, and predictive systems add an extra dimension to perimeter protection by enabling a proactive rather than reactive response.

Biometrics technologies are being embraced in video analytics particularly as we approach the limits of human operators. Human concentration, which can taper off after 20 minutes, means that

[4] https://ww2.frost.com/news/press-releases/frost-sullivan-biometrics-can-be-alternative-conventional-authentication-technologies-mobiles/

[5] https://www.forbes.com/sites/stevemorgan/2016/01/24/how-consumers-lost-158-billion-to-cyber-crime-in-the-past-year-and-what-to-do-about-it/#2b6559a2b655

human operators tend to have a high rate of overlooked events, especially when bored or fatigued. Furthermore, relying on human surveillance is not only inherently inefficient, but also increasingly expensive as manpower costs continue to rise.

Then there is the challenge of dealing with the sheer volume of video data being generated. Video surveillance is predicted to reach a staggering 3.3 trillion hours of video in 2020, according to a report by Homeland Security Marketing Research[6].

Going by a conservative assumption that only 20 per cent of the most critical video will be reviewed by staff, this nonetheless entails a workforce of over 110 million security personnel worldwide, dedicated to video surveillance.

Not only will video analytic systems be inevitable, but they will also bring new capabilities to the table. Motion detection can be used to identify behaviours such as loitering or objects that have been stolen or left behind.

These capabilities will be particularly useful in high security areas such as airports, alerting staff to suspicious persons and objects such as unattended baggage. Video analytics are also able to automatically track moving objects across multiple cameras and give real-time information on the movement of crowds.

> “Human concentration, which can taper off after 20 minutes, means that human operators tend to have a high rate of overlooked events, especially when bored or fatigued.“

The ability to sharpen images from low resolution video and the automated filtering of irrelevant images facilitate forensic video searches and post event analyses. For example, individuals identified by video surveillance can be checked against Interpol’s stolen and lost passports list.

Video analytics is not restricted to facial recognition, but has also been very useful in vehicle and license plate recognition for security purposes.

MULTI-MODAL BIOMETRICS

Although biometric technologies are a vast improvement over existing identification and authentication methods, no technology is infallible. Though the chance is small, errors could potentially be introduced at each stage of the biometrics process, from enrolment and matching to database management.

Apple’s TouchID system was shown to be hackable within hours of its 2013 launch. Using a latent print from the phone, a laser printer, some white wood glue and a bit of breath to keep the fake print moist, the Germany-based Chaos Computer Club was able to bypass the fingerprint lock screen[7].

There are situations in which single parameter biometrics fail. For example, two to three per cent of the population have no usable fingerprint, such as laborers with worn fingerprints or people with a genetic condition called adermatoglyphia, also known as immigration delay disease.

Clearly, no single biometric parameter is perfect; each has its own advantages and disadvantages in terms of ease of capture, performance and cost. To get around these issues, multi-modal biometrics has been employed, where two or more sources of biometric information are captured and used to cross reference each other.

While it may be possible to fool a single biometric reader, it takes much more effort to hack into a system which uses multiple biometric readouts. In the previously mentioned Aadhaar program for example, all ten fingerprints as well as a photograph and two iris scans are taken, making the system more robust.

Of course, increasing the number of biometric parameters captured also increases the cost and complexity of implementing the system. Rather than use the maximum number of biometric parameters for every process or transaction, single factor biometrics could be used in parallel with traditional measures such as passwords or tokens, enhancing instead of replacing them.

For high value transactions, where the higher costs are offset by the higher risks, a multi-modal approach could be used. This layered system would help to keep costs low and increase the speed of biometric clearance.

MOBILE BIOMETRICS

There is little doubt that the field of biometrics will continue to grow, spurred by both large government projects and wide-scale adoption by individuals. Of these two forces, personal adoption, and mobile biometric technologies are likely to shape the face of biometrics of the future.

With the ubiquity of mobile devices today, it is easy to take for granted the technology that has driven the mobile revolution. Each smartphone has processing power that was unattainable by desktop computers a generation ago crammed into a handset that fits into a pocket.

The integration of biometric and mobile technologies will lower infrastructure costs and help to take biometrics to where the people are. Mobile-enabled biometrics can be used in remote locations; anywhere with an Internet connection.

The greater convenience afforded by biometrics could go a long way in enhancing mobile security, where typing complex passwords has been met with resistance, a serious issue for companies adopting Bring Your Own Device (BYOD) policies.

[6] http://www.homelandsecurityresearch.com/blog/global-video-analytics-market-to-triple-over-the-next-decade/

[7] https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands

BIOMETRICS ON THE MOVE

Enabled by the latest advances in capture technology, biometrics on the move allows features to be taken without manual intervention and even while the subject is in motion. Also known as stand-off biometrics, this technology enables contactless fingerprint capture and iris or face detection based on video surveillance.

In contrast, older technologies are cumbersome and time consuming, requiring direct contact with a fingerprint scanner or for the subject to present themselves to the capture device, holding still to ensure a high-quality scan.

Biometrics on the move could potentially revolutionise law enforcement, allowing real-time watchlist detection and monitoring of people moving through sensitive areas such as nuclear power plants and security facilities. In public safety, biometrics on the move could help with crowd control and flow management, automatically preventing bottlenecks which could potentially be dangerous or at the least, time wasting.

Biometrics on the move also finds many applications in providing business intelligence. Anonymous, non-intrusive real-time monitoring can capture "soft" biometric features such as age, gender and ethnicity, allowing retailers to provide targeted services dependent on demographic features. Information on the people walking through a mall, for example, could help retailers make decisions about how to design and stock their stores.

Most of all, biometrics on the move makes the adoption of biometric technology convenient for users. For example, it can be used to capture information of passengers as soon as they walk into the airport, reducing the amount of time spent clearing immigration. Biometrics embedded in the environment go one step beyond mobile solutions, seamlessly integrating technology into everyday life.

CASE STUDY

HOW THE AIRPORT OF THE FUTURE CAN MAKE USE OF BIOMETRICS FOR FASTER, SAFER TRAVEL

From the moment a passenger steps into the airport to the time he boards the plane, he can go through automated self-service processing and avoid long queues. The authorities would also not be required to repeatedly verify him at various checkpoints, thus removing bottlenecks in the process.

Here's a typical journey through the airport:

1 ARRIVAL

A passenger first arrives at the airline counter to check in, if he has not done so previously.

He goes through existing procedures, possibly at a self-service kiosk, to confirm his check-in and drop off his bags.

TO THE SECURE AREA 2

At an integrated biometric clearance gate, he presents his passport and boarding pass and performs a name match and tags his passport with a seat number.

Here, he also scans his face and has the live image compared to either the data on an e-passport or a regular passport photo. Where needed, he could be asked to scan his fingerprint or iris for a second check required by local immigration authorities.

3 BOARDING

At the boarding gate, he scans his boarding pass at another automated e-gate for passenger reconciliation.

His live face image is again checked against the photo collected at the earlier immigration e-gate. The transaction is logged, then the face image is deleted to preserve the privacy of the individual.

CHAPTER 5

Face Recognition

Once written off by early adopters, face recognition has come a long way to become a vital component in today's security and commercial landscapes.

A face remains the most widely used way of identifying or authenticating a person. A photo of it is on most identification documents that we carry in our wallets. A lot of information can be provided from a person's face, clothing, and appearance, and today a person's face has become the epicentre of the most fascinating and promising evolving forensic technology – face recognition.

In the field of biometrics, perhaps nothing stirs up as much debate as face recognition. Using technology to identify or verify a person has always been something easily understood in theory. Heavy use of such technology in Hollywood blockbusters like Minority Report has certainly helped the technology gain widespread exposure among mainstream audiences.

While humans have always had the innate ability to recognise and distinguish between faces, computers only recently gained the same ability. It is still improving rapidly today, but from the time it was first worked on in laboratories in the 1960s, the technology has advanced by leaps and bounds.

In 2006, a test of several face recognition algorithms by the National Institute of Standards and Technology (NIST) showed that machine recognition has improved tenfold since 2002 and a hundredfold since 1995[8]. The best algorithms actually performed more accurately than most humans can manage.

That was in 2006. Since then, face recognition has been one of the most progressive technologies in the world, thanks in part to new methods of measuring up a face.

In 2017, NEC's face recognition technology had an accuracy of 99.2 per cent when it comes to detecting the right person at an airport passenger gate. This was confirmed in NIST's tests that were conducted to recognise one individual at a time as they walked through an area without stopping or acknowledging the camera.

[8] https://www.technologyreview.com/s/407976/better-face-recognition-software/

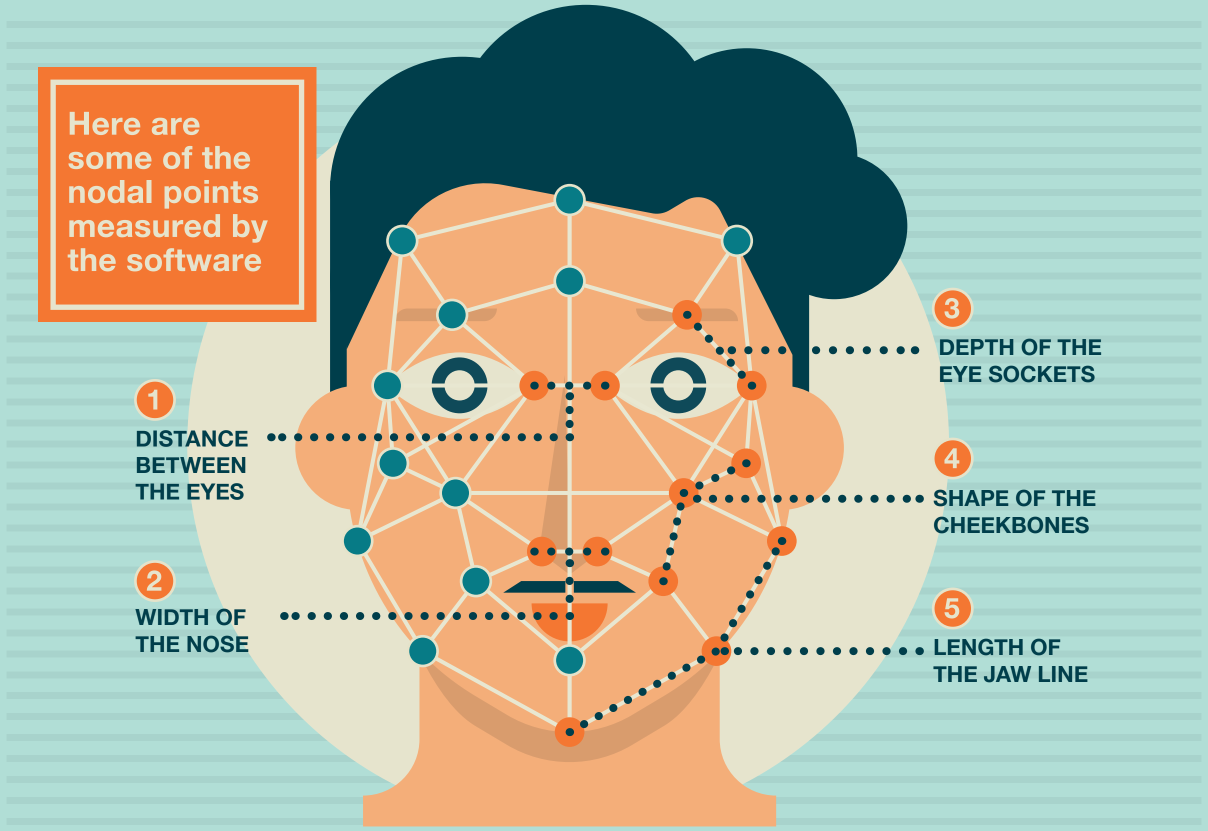
UNDER THE HOOD:

HOW FACE RECOGNITION WORKS

Once it detects a face, a face recognition system determines the head's position, size, pose, and unique characteristics.

Every face has numerous, distinguishable landmarks — the different peaks and valleys that make up facial features. These landmarks are called nodal points.

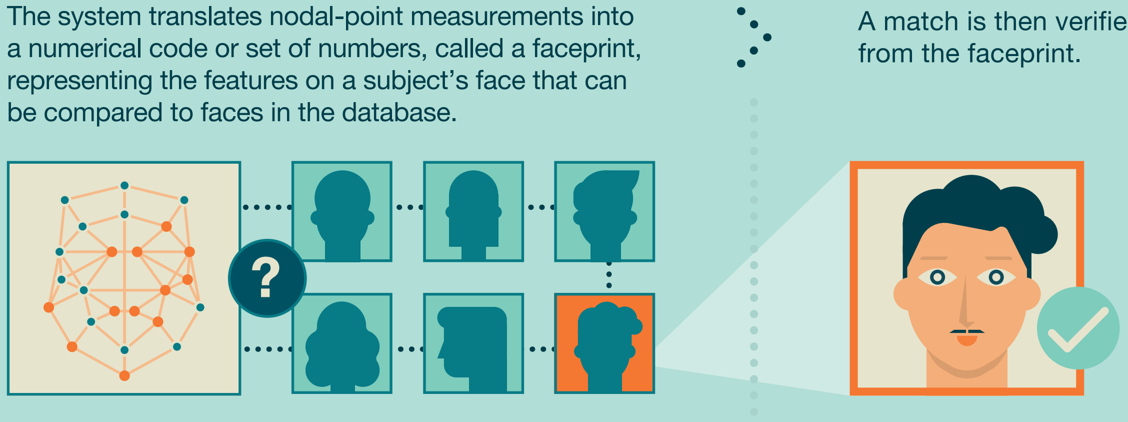
EACH HUMAN FACE HAS APPROXIMATELY **80 NODAL POINTS**



Here are some of the nodal points measured by the software
1 DISTANCE BETWEEN THE EYES
2 WIDTH OF THE NOSE
3 DEPTH OF THE EYE SOCKETS
4 SHAPE OF THE CHEEKBONES
5 LENGTH OF THE JAW LINE

The system translates nodal-point measurements into a numerical code or set of numbers, called a faceprint, representing the features on a subject's face that can be compared to faces in the database.

A match is then verified from the faceprint.



FACE-TO-FACE WITH THE TECHNOLOGY

In the past, many algorithms relied on 2D measurements between a person's eyes. Despite this being a sensible method, results can be profoundly affected by the angle of view or a different facial expression. Even the smallest changes in light or orientation can reduce the effectiveness of a system, rejecting a match to any face in the database, and leading to a high rate of failure. Face recognition technology today can check on a wider number of features.

Today, face recognition technology uses advanced pattern recognition models and captures images in real time to select areas of the face with dense information values — such as the curves of the eye socket, nose and chin — to identify the subject.

These areas are all unique and do not change over time. Face recognition today can even be used in darkness and has the ability to recognise a subject at various view angles. These are just among some of the many features that have come to define the technology in recent times.

To achieve reliable face recognition of a video image, NEC developed feature-point extraction technology that enables enhanced face recognition to a level where an individual can be identified with high precision from within a group, even if their face is partially hidden, or the image is taken from different angles.

NEC's face recognition technology also uses deep learning technologies for face matching to increase accuracy to a level where an individual can be identified by a low-resolution face image captured by a distant camera.

These enhancements helped NEC come out tops in a comparison of various vendors' technologies in NIST's 2107 Face in Video Evaluation (FIVE) test. NEC's solution was both fast and accurate, two important qualities that are needed for real-time use cases.

It is also a sign of how far face recognition has come. Back in the early 2000s, several early and high-profile installations, by police and airport authorities, for example, were scaled back because of a lack of accuracy. Today, as the technology has improved, so has the acceptance.

GOING BEYOND CONVENTIONAL SECURITY

Previously built with the vision of improving security within the law enforcement space, the breakthrough in face recognition now sees the technology being applied within a larger audience. On top of providing enhanced security today, the technology has proven to be versatile enough to be deployed across areas of financial services, entertainment, advertising and many more.

Banks, for example HSBC in London, use face recognition to enable authorised users to enter a secure vault. This method of authentication is not only easy to use, but also highly accurate and secure.

Credit cards can also be protected by the safest, most user-friendly authentication available–the owner's face. A person paying for items at a cashier can be verified by a camera connected to a face recognition system. Pass the "face test" and the payment goes through.

Increasingly, too, companies are seeking to deploy face recognition to know customers better and provide improved service. Commercial uses, such as for customer service management, queue monitoring or business intelligence, are now benefitting from the advances in face recognition in recent years.

In London, retailers have used a face recognition solution from NEC to identify its loyal or VIP customers walking into a store. A camera picks up the image, which a computer then compares against a database. When a VIP walks in, a sales assistant is quickly alerted to provide more personalised service to him.

In Osaka, the Universal Studios theme park uses face recognition to identify annual pass holders. This allows the holders to enjoy a VIP experience without requiring additional paperwork.

These are but a few examples of what face recognition can offer in the coming years. With vast amounts of data collection, storage and crunching that is made available through the use of cloud technologies, it is going to provide even more insight for organisations interested in both commercial and security applications.

Here's a look at four scenarios where facial recognition may be deployed.

1. CONTROLLING ACCESS

Comparing a person's face with a photo ID is one of the oldest ways to verify if he can enter to a restricted place. Now, face recognition just makes that task much easier, allowing security staff at border control or even a casino to prioritize on other duties such as identifying potential offenders based on their behaviour.

In Canada, the Ontario Lottery and Gaming Corporation has been turning to face recognition to automatically recognise some 15,000 self-identified problem gamblers–and keep them away from its betting tables.

Cameras photograph everyone who walks through the front doors of a casino, which gets 40 million visits a year. A computer then compares the images against a database of individuals who have put themselves on a self-exclusion list.

If a match is found, security guards are alerted via a silent alarm. They then carry out a manual comparison and approach for identification. If the match is confirmed, the person is escorted out of the casino.

Privacy safeguards are in place as well. The photographs of people who don't match any images on the database are discarded. Those in the database are biometrically encrypted and only decrypted when a person in one of the pictures is present.

In the same way, face recognition can be used for border control. Canada, incidentally, is also one of several countries to issue e-passports with a smart chip that can be used with face recognition technology. This allows officers, possibly in future, to compare a physical person's appearance with a digital photograph that is stored on a chip and not easily faked.

2. FINDING SUBJECTS IN LAW ENFORCEMENT

In the security and law enforcement sectors, the usage of face recognition is arguably the most obvious – and often accepted – to most citizens in a smart, connected city.

The technology can be used to identify, for example, known suspects who are the subject of a police investigation. To do this, law enforcement agencies would have to not just collect thousands of images – both video and still images – but also to analyse the information within the tight time frame available to solve a case.

In the United States, the Federal Bureau of Investigation (FBI) is spending US$1 billion in a Next Generation Identification (NGI) program, which will add biometrics such as iris scans, DNA analysis and voice identification, along with face recognition, to an investigator's toolkit.

There are several possible use cases. Law enforcement agents might try to identify fugitives or missing persons from a face recognition database. They may also do so for unknown persons of interest. Using sophisticated multi-camera technology, they may even track subjects moving from one place to another after a critical incident.

If agents already have a suspect, they may also look out for someone they'd expect to turn up at a certain place, such as a crowded stadium. Conversely, if a riot had happened at a stadium, investigators could look at the video footage to identify who the rioters were.

The technology is already there now. The challenge is to identify subjects from a fast-growing database of photos and videos. Sometimes, face recognition is one clue in a digital trail left by a subject, for example, when he makes a call or uses a credit card.

To tap on a multi-modal database of information, many law enforcement agencies are looking to cloud-based solutions, where storage and computing capabilities are on tap should an investigation scale up.

3. IDENTIFYING CUSTOMERS

A relatively new use of face recognition is in the retail space. This enables companies to quickly and seamlessly identify a frequent customer, and ensure that he or she gets personalised service without having to explicitly disclose his or her identity to the shop assistant.

A camera at the store captures images of everyone stepping inside, then sends the data to a remote computer that compares them against a database of known VIP customers. Various measurements of the face are taken and checked against a template. If a match is found, usually within a split second, the sales assistant is alerted on the smartphone or iPad to provide personalised service. He or she would also be fed details such as the customer's dress size or other preferences gleaned from previous purchases.

Already, a dozen top stores and exclusive hotels in Britain, America and Asia have been testing the face recognition technology provided by NEC. It works even when people wear sunglasses and other items that cause other face recognition technologies to stumble.

Because NEC uses a holistic method of combining various ways to detect a face, it works similarly to how a person would identify another. Just like how we may recognise a friend wearing glasses or with a slightly new haircut, the system is able to adapt to these subtle changes and correctly recognise a face.

4. PUTTING MORE THAN JUST A NAME TO A FACE

Regular customers, of course, still count. Retailers can now "see" every single customer who walks into and uses that image data to estimate the typical gender and age of their clientele. All they need now is a camera, PC and a subscription to NEC's cloud-based face recognition service.

Leveraging on NEC servers on the Internet, the service takes images sent from a merchant and does the analysis off-site, saving merchants the heavy investments required to deploy the technology themselves. The service costs 70,000 yen (US$880) a month in Japan and has been running since its launch in 2012.

The use of such face recognition technology extends beyond retailers. Large malls, for example, could accurately determine the type of crowd it attracts in certain times of a day at certain parts of a complex.

The same technology could be used in interactive advertisements, which can estimate the age and gender of a person in front of them. The messages can then be customised to fit the person, resulting in a more effective pitch.

Ultimately, with intelligence gleaned from actual customers and users, retailers and advertisers can better strategise marketing plans to target the right demographic groups.

ENSURING PRIVACY IS PROTECTED

All the good technology cannot be used if organisations rolling out face recognition in their operations do not get the critical buy-in from users themselves.

Unlike fingerprints, it is easy to capture an image of someone's face without consent. That is a double-edged sword. Face recognition is often viewed as a "contactless" form of surveillance, identification and verification, which makes many people understandably concerned, especially about preserving their anonymity in public.

In the recent years, Facebook's controversial deployment of face recognition technology to identify people in uploaded photos and even law enforcement efforts to capture and analyse publicly available images have also met with privacy concerns.

These are key issues to address should face recognition be adopted by organisations in both public and private spaces. What is important is not just the capturing of such information, if it is in public or clearly shared by a user, but the design and governance that come with storage, access and analysis of such personal data.

The Federal Trade Commission put out a staff report in 2012[9], where it listed some best practices that organisations can put in place. For example, companies that hold databases of consumer images should design their services with privacy in mind. Should the images be no longer needed, they should be deleted. If retained, they have to be reasonably protected.

Transparency to end users is another key point. Organisations deploying face recognition in digital signage, for example, should make clear to users that they are being observed, since they may not detect a camera in the setup.

Yet another issue brought up by the report concerns social media networks. Without a consumer's consent, they should not identify him to someone who would otherwise not be able to identify him. For example, a mobile app that lets a person identify another at a bar, with possibly added information such as his address, could raise safety risks and only be allowed with the user's consent.

[9] https://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy

FOUR FACTORS TO CONSIDER

When governments and commercial organisations decide to turn to face recognition technology, a number of questions come up often. Here are four that should be asked of a vendor proposing a solution.

1. How fast, accurate or reliable is it?

Independent tests provide a good gauge of how good a face recognition system is, and NEC has regularly come up tops in tests in the United States.

In 2009, NEC's face recognition technology was ranked number one in the Multiple Biometric Grand Challenge's (MBGC) "Still Face Challenge", carried out by the National Institute of Standards and Technology (NIST) and commissioned by the United States Department of Homeland Security. In 2010, NEC again achieved the highest score in the new Multiple Biometric Evaluation or MBE 2010 benchmark.

NEC's technology is also often seen as holistic. It takes a number of methods to recognise a person, thus overcoming common issues like a unique facial expression or a pair of sunglasses blocking key features. Like how a human recognises another, our solution uses various methods to identify a person, bypassing problems that usually fool other systems.

2. Does the face recognition require specialist, expensive cameras?

Some face recognition solutions are highly accurate only when fed high-resolution images taken by expensive, specialist cameras. This not only requires a heavy investment to cover a large area, but also makes existing cameras unusable.

NEC's solution works with a diverse range of image sources, including live cameras. The resolution required for an accurate identification is also modest, making our solution a good fit in a city with various types of camera systems already in place.

3. Does the vendor provide a way to store and analyse the images on-demand, and provide the scalability in a time of urgency?

All the information in the world is useless unless it can be accessed to provide timely insights, say, during a critical event. While many vendors provide face recognition as a standalone service, NEC's face recognition solutions are part of a globally-trusted portfolio of biometric and safer cities solutions. From providing multi-modal forensics to cloud-based solutions, NEC backs up its face recognition solutions with tried and tested capabilities in related areas.

4. Is the technology open or locked in for future upgrades?

This is key to organisations looking to build a system that can be upgraded in the years ahead, as face recognition technology is improving all the time. NEC's system is flexible in the way it works with other installations. It also plugs right into our safer cities solutions, which optimise results in face recognition by making use of its findings in various related scenarios.

CASE STUDY

HOW FACIAL RECOGNITION IS CHANGING THE GAME IN COLOMBIA, WHERE BAD ELEMENTS ARE KEPT OUT OF A STADIUM

There are two big teams in Medellin and each one is supported by very passionate fans. Just like in any football-mad city in Latin America or Europe.

And like the rivalries in many other places, people can go overboard when that rivalry turns ugly. Unfortunately, this fierce rivalry sometimes results in violence during match days, when fans turn on each other when the match is going on.

While most people in the Atanasio Girardot stadium are there to enjoy a match and not stir trouble, there are small groups of hooligans who wish to resort to violence. This causes not only damage to the stadium but also injuries to innocent match-goers as well.

1 VIDEO SURVEILLANCE

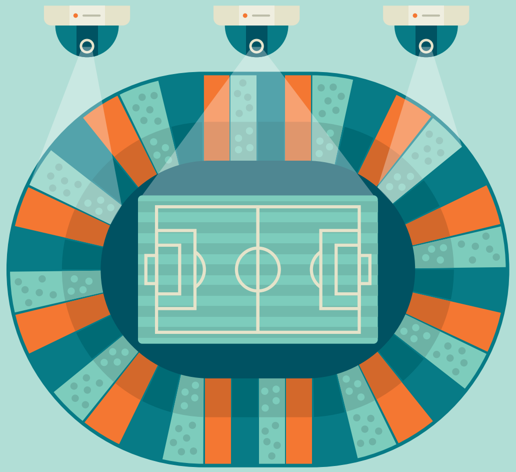
The city authorities turned to NEC's NeoFace Watch to identify the football fans entering the stadium.

This forms an important part of the video surveillance system there.

2 PHOTO CAPTURE & REGISTRATION

The stadium now has 170 specialty cameras.

Of these, 50 cameras located at the entrances and 25 higher resolution cameras for the grandstand. On top of this, there are 55 cameras that are fixed or can pan, tilt and zoom around the stadium.



This helps capture images of people in the stadium which can be checked against a database of enrolled fans.

These fans have had a photo taken and provided basic personal data and been approved earlier in a registration process that takes half a minute. There are also eight enrolment stations at the stadium, so people can get registered on the grounds.

3 WHITELISTING & BLACKLISTING

From here, the stadium staff can create a whitelist, allowing identified football fans to enter.

At the same time, those with a record of violence in the past can be barred from entering. Inside the stadium, the cameras help identify a person involved in a violent act, identifying him and potentially barring him from entering in future.

4 SEND ALERTS TO STAFF

If a person in the stadium is identified as someone on a blacklist, the stadium staff receive e-mail or SMS alerts, advising them to take action.

CHAPTER 6

The Role of IoT and AI

No longer just science fiction, the Internet of Things and artificial intelligence are important technologies in ensuring safety in a digitally connected city of the future.

From world-beating chess machines to self-driving cars, artificial intelligence (AI) has captured the imagination in recent years. What was once science fiction has begun turning into science fact of late.

At the same time, the Internet of Things (AI) is abuzz with an increasing number of sensors and data collection points, ranging from the smart devices carried and worn all the time by users to cyber sensors that watch for unusual online traffic in a network.

Together, AI and IoT have the potential bring about a dramatic transformation in the quality of life for citizens in a smart city. By merging the physical with the cyber, the connectivity among real world objects and people in an urban environment is closer than ever.

The knowledge arising from the Big Data generated each day – from the health statistics collected by a smartphone user to the stress levels on urban infrastructure such as subway train tracks, for example – is unprecedented.

The amount of digital data generated in a year is growing from 4.4ZB in 2013 to an estimated 44ZB in 2020, according to research firm IDC[10]. That represents a growth of 40 per cent a year.

With that data, many smart city solutions can be developed. From ones that find the best routes for garbage trucks in a neighbourhood to those helping city planners determine where to locate factories away from residential areas, fresh insights can be derived from the data are growing.

This is helped by increasingly sophisticated AI. With machine learning, it can find new patterns and logic, zeroing in on an answer to a tough question, say, the optimal way to transport the largest amount of people during peak hour with the smallest carbon footprint.

Indeed, by melding the physical and cyber worlds, city leaders are increasingly able to plan and optimise the way their city is run. In a digitally connected society, the benefits to citizens are clear.

[10] https://www.emc.com/infographics/digital-universe-2014.htm

THREATS TO CYBER AND PHYSICAL WORLDS

At the same time, as opportunities flourish for citizens, so will openings be created for cyber criminals and state-sponsored threat actors. As more facets of a population are available digitally, the risks faced by citizens are higher as well. While remote access to the physical world may bring convenience, it also enables cyber attackers to gain easier access to critical systems.

In 2010, the world caught a first glimpse of Stuxnet, a malicious programme customised to attack the industrial systems used to operate Iran's nuclear programme. It looked for certain control systems in a nuclear plant, then changed the settings to sabotage them.

Believed to be written by state-backed authors, the software has been taken apart and reworked by others so it can now cause more damage elsewhere on machines that are not protected.

In the years since, the sophistication of malware targeting industrial systems, often those controlling critical infrastructure such as power plants or telecom networks, has only increased.

At the same time, the setting up of IoT and digitalisation of business processes have meant more connected systems over the past three years. While many also have more security in place today, the digitalisation and "sensoring-up" of systems may provide an attacker with a way to create major damage should he be able to connect to these systems remotely. This could be carried out through an exploit from other connected systems, for example.

Alternatively, an attacker could choose a softer target to create mayhem in a city. In a rush to deploy sensors and connected devices in the city, many planners may not have had set up an adequate level of security in place to prevent them from being hijacked.

One of the biggest distributed denial of service (DDoS) attacks in late 2016 occurred with the help of thousands of CCTV cameras and digital video recorders taken over by hackers.

These devices were targeted by a malware called Mirai. It looked for devices that had factory-default usernames and passwords, which were then used to send massive amounts of traffic towards an online target to flood it and knock it out of action.

The attack in October 2016 caused massive outage on the Internet, preventing many users from reaching sites and services hosted on popular cloud platforms, such as Twitter, Netflix, Spotify and Amazon.

> "As cities and homes become more digital - from using smart kettles at home to setting up flood detection sensors in storm drains - answering the need for stronger security has to be a top priority."

For many security experts, the attacks are a wakeup call that is long overdue. As cities and homes become more digital – from using smart kettles at home to setting up flood detection sensors in storm drains – answering the need for stronger security has to be a top priority.

Unfortunately, there are already millions of cameras and other connected devices already in the open. Many will still have their passwords unchanged, while others cannot be patched up to prevent future attacks because their manufacturers may not offer the updates.

The potential for a DDoS attack, possibly against a city's critical infrastructure, has to be taken into account as more IoT devices come online. In an interconnected world with no borders to prevent such cyber attacks, it is imperative that governments work closely together to tackle such threats.

One of the biggest challenge today for IoT has to do with securing the devices. Increasingly, city planners connecting up their environments have to consider sensors that have security built in. They have to be able to deliver the data they collect securely and be resistant to being hijacked for a DDoS attack on other parts of a city.

As the cost of IoT sensors fall, as with the maturing of technologies, the emphasis of many vendors is on "baking in" security in the hardware itself. This will make each connected Thing on the network a lot less susceptible to be taken over for malicious purposes.

AI AND IOT FOR A SAFER CITY

Keeping IoT devices secure is a top priority because these devices can also help detect unusual phenomena in the physical world. The warning they provide can make a difference during an emergency.

For example, a sensor that detects air quality may be able to pick up an unusual particle in the atmosphere that may signal a chemical agent being released in a terrorist attack.

Individual sensors worn by users may also come in use, for example, in sensing a major event. In 2014, during an earthquake in California, wearers of fitness trackers were awoken in their sleep in the middle of night. This caused a spike in the percentage of people awake suddenly at the same time, as recorded on their personal devices[11].

The key in future could be finding a way to harness the continuous stream of data users might want to provide to enhance the security of the city they live in. Drivers in Singapore can now volunteer to share videos they record in their car cameras with the police to collect evidence for a case[12].

Smartphones in the hands of members of the public are also important in the event of an emergency. A police app lets citizens easily send videos and pictures to the authorities, say, if they see a suspicious person in public. The increasingly powerful sensors in personal devices make this a new avenue that the authorities can seek greater citizen involvement in.

For this to work, all the data that is coming in has to make sense to the human operator or city leader. During a crisis, he has to be presented with a clear picture of the most important things happening, while having the noise reduced.

This is where AI will play a growing role in the future of safer cities. Facing attacks that may not come from traditional sources or follow familiar patterns, the deep learning that AI is capable of now can quickly assist in deciphering a situation.

Already, AI-driven image analysis now enable law enforcement and homeland security forces to track persons of interest across different locations that utilise different camera systems. Coupled with other command and control systems, the autonomous system can more easily identify and monitor a suspect over vast stretches of physical space – every time he steps into the eyes of a camera.

In the digital realm, AI is making an impact in cyber defence as well. In fighting off future threats, the priority today is not simply looking for known threats but also what is unknown. Zero-day vulnerabilities, the newfound loopholes that expose systems to attackers, are often the weapon of choice of many sophisticated threat actors today.

What is required to counter threats that one may not have faced before is to look out for tell-tale signs of a possible penetration or impending attack. With AI, a defence system filters out the "safe" or normal signs of everyday activity and focuses on actions or behaviour on a network that may point to an infiltration.

The system also unburdens the human operator from false positives. If a sensitive cyber defence mechanism triggers too many false alarms, it may end up being ignored when a real threat occurs. With AI, the system learns what appears to be regular activity and flags actions that may lead to a security breach, for example, someone copying large files from a server onto a USB drive then deleting the files on the PC.

In a inter-connected city, AI is the smart defender needed to pre-empt attacks, guarantee the certainty of information and carry out secure hardware development. And as the arms race with cyber attackers continue in the coming years, smart cities also have to evolve their defences by tapping on more sophisticated AI.

AI, after all, has been through three big leaps over the past six decades. In the 1950s, the early version was more akin to solving a "toy problem", where humans had to tell the machine what exactly to do. In the 1980s, as computers became more complex, users could put together a set of rules and let it follow them to find a solution.

The current iteration, in the form of machine learning, is one where AI is able to derive rules from sets of data given to it. So, by repeatedly showing a machine, say, thousands of images of a cat, it will find the patterns to the object and deduce that there may be, say, a 90 per cent chance an image of a cat is indeed one.

However, there is still a limit to the understanding that a machine can have. Researchers have, for example, added noisy pixels to adjust just 1 per cent of an image and a computer would wrongly identify an object, even though the image still looks pretty much the same – of a cat – to a human.

The next big step is for a machine to not just recognise patterns but understand and explain that a cat is identified by its whiskers, face shape, colour and other features. In other words, it works more like a human mind. It will not just be able to identify a pattern but also understand the reason why it can identify it, then repeat that learning to find new patterns.

This means it can set its own rules for cognition. It may be able to identify an object faster, for example, like a human child who can recognise a cat without having to be shown 10,000 images of it. The capacity for deep learning may characterise the next big leap for AI, something that researchers are still striving to achieve today.

For smart cities, the implications are tremendous. The rapid developments of AI, coupled with the learnings for both man and machine in the field, mean that they will shape the lives of citizens in future in more ways than many recognise.

For city planners, taking AI onboard early today means reaping the benefits early. From making sense of all the data coming in from a network of sensors and devices to developing stronger defences against complex threats of the future, it is a crucial technology in a safer city.

[11] https://jawbone.com/blog/napa-earthquake-effect-on-sleep/
[12] http://www.straitstimes.com/singapore/submit-clips-of-road-offences-to-us-traffic-police

CHAPTER 7

The Future Looks Bright

Safer city technologies are making a real difference today and will have even greater impact on citizens in the years ahead.

In the years since the first seeds of a smarter, safer city idea were sowed in the minds of forward-looking city planners, it has developed into fully functional rollouts that are impacting the lives of citizens every day. Even as smart technologies evolve and face challenges at the same time, they are moving forward as innovation is coming off laboratories and being tested in real-world scenarios all the time.

In Singapore, a trial is ongoing to link all citizen data to a single government repository. This way, they don't have to key in the same personal details when dealing with different agencies, say, the taxman or the public housing board.

The country is also looking to create a digital ID system that can offer an alternative to physical identification cards. This secure online system will enable users to log in to services on the Net safely and identify themselves to the government to transact with various agencies.

Elsewhere, technologies that have been proven in independent tests and have extended their impact globally. NEC's NeoFace Watch, for example, is being deployed in a growing number of uses.

At airport terminals, the face recognition technology recognised by independent tests as the fastest and most accurate around is scanning faces each day to let through authorised travellers. At stadiums, it looks out for people who are on a ban list for previous hooligan behaviour and prevents them from entering and disrupting a game for other fans.

Increasingly, the NeoFace Watch technology is also being used in searches for persons of interest based on even the most blurry, low-resolution and imperfect images from old surveillance cameras. It is just one example of a technology that is expanding in its scope as smart cities grow more sophisticated and complex.

Making sense of all this is increasingly becoming difficult for humans. The biggest development in years is set to be AI. Instead of the early versions where computers were given instructions to follow rigidly, today's deep learning machines are able to learn and react to situations much faster than humans – even in a way and at a pace beyond what their creators are able to understand[14].

With so much information coming from IoT sensors around the world, the raw data has to be analysed and made sense of. Only with sophisticated AI can that be transformed into actionable intelligence that human operators can use.

The worry for AI – and indeed smart technologies in general – is the push-back from users who may feel their lives are being invaded. From smart TVs to social media, people are fearing a lack of control over their own information and how it is being used against their wishes.

Indeed, so-called neo-Luddites are seeking to unplug and avoid being part of the digital grid that is growing more pervasive by the day[13]. Often tech-savvy users, these small groups seek to depart from the network of users that everyone else is plugged into.

Though the movement is a small one, the worry they feel resonates among most digital technology users. From people worried about their phones being tracked via an app[14] to the increasingly common ransomware threats, there are challenges that smart city planners have to overcome.

Key to this is the issue of privacy. While some jurisdictions such as the European Union has strong data protection regulations against the handling of individuals' personal information, other places may not have the same level of protection.

At the same time, many users still want the authorities in charge of a city to take care of their information, since they have to use that to transact for all manners of services, from paying taxes to seeing a doctor.

> "This means the challenge for smart cities is two-fold. They have to move fast enough to bring clear, immediate impact to citizens, while avoiding the pitfalls of not paying attention to their privacy concerns and the importance of cyber security."

This means the challenge for smart cities is two-fold. They have to move fast enough to bring clear, immediate impact to citizens, while avoiding the pitfalls of not paying attention to their privacy concerns and the importance of cyber security.

For many countries seeking to implement a smart project to address a particular issue, such as safer living environments, the approach has to be holistic. In other words, they have to consider the impact of the solutions they are implementing. They have to look beyond the technology.

In Singapore, one of the most prominent smart nations of the world, the pace of development has not been deemed fast enough[15]. It is seeking to change lives more dramatically and transform many processes that citizens have to go through to interact with the government daily.

Singapore's experience is from an early adopter and global leader of smart city technologies. As a testbed, it has learnt valuable lessons on rolling out such innovations in future. It stands in front of others which are starting to get into the game today.

At the same time, the learning curve in Singapore is also steeper than it had expected. Various agencies each with their own camera networks, for example, could share data more readily if their systems were better connected. A more integrated approach might accelerate the takeup and development of a smart city deployment.

Another important point it will share is that any sort of transformation has to be citizen-centric. In other words, the focus cannot be on technology, as many initial smart city rollouts have been about, but on the end user.

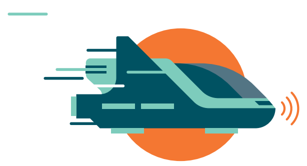
Buy-in is an important element in the success of a smart city deployment. In Singapore, for example, old folk were placing towels over sensors meant to monitor their safety at home, because they preferred their privacy and independence[16].

What proponents had to convince users were the benefits they would enjoy with the new technology. In other words, could they have asked users what they wanted to achieve with the sensors or smart technologies so they would willingly be part of a programme[17]?

In various rollouts around the world, this is turning out to be true. In Copenhagen in Denmark, for example, cyclists ride to work each day with sensors on their bikes to give feedback of the road conditions so they may be improved in future. At the same time, the sensors provide weather information for the rest of the city so they can benefit from the effort as well.

Ultimately, users will dictate what smart technologies might be successful in future. City planners will find that services that are adopted most widely are the ones that make the most sense to citizens. This means they may have to plan deployments based on needs rather than technological trends.

This is a departure from the sentiment a few years ago, when innovations such as AI and IoT were just emerging with the promise of delivering a higher quality of life to citizens. Now, as they mature, and as real-world deployments provide valuable user feedback, cities have to do more to the next step. This means matching smart technologies to needs.



[13] PENDING
[14] https://www.nytimes.com/2017/04/23/technology/travis-kalanick-pushes-uber-and-himself-to-the-precipice.html
[15] http://www.pmo.gov.sg/newsroom/dialogue-pm-lee-hsien-loong-camp-sequoia
[16] http://www.straitstimes.com/singapore/untangling-the-way-to-a-smart-nation
[17] https://www.techgoondu.com/2017/03/29/time-government-agencies-citizen-centric-singapores-smart-nation-push

ANNEX: A CITY PLANNER’S GUIDE TO PUBLIC SAFETY

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 have to develop its own solutions, tailored to its specific context and needs.

Technology can play a significant role in helping cities respond to security challenges. There are seven key public safety areas for every city, which city planners have to address:

They are: citizen services & immigration control, law enforcement, critical infrastructure management, public administration services, information management, emergency & disaster preparedness and lastly, inter-agency collaboration

1. Pinpointing Identities

with Citizen Services and Immigration Control

Opportunities and threats alike thrive in today’s globalised 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 travellers.

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 travellers.

2. 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.

3. 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.

4. 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 the outbreaks of bird flu and SARS in recent years, 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.

5. Ensuring Digital Security

with Cyber Security

As 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.

6. 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.

7. 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.

REFERENCES

1. United Nations World Cities Report 2016.
https://www.techgoondu.com/2017/03/29/time-government-agencies-citizen-centric-singapores-smart-nation-push/

2. The cost of ransomware attacks: S$1 billion this year.
http://www.zdnet.com/article/the-cost-of-ransomware-attacks-1-billion-this-year/

3. The Internet of Things: Sizing up the opportunity
http://www.mckinsey.com/industries/semiconductors/our-insights/the-internet-of-things-sizing-up-the-opportunity

4. Iranians travelling on flight MH370 forged passports ‘not linked to terror’
https://www.theguardian.com/world/2014/mar/11/passengers-malaysian-plane-mh370-iranian-forged-passports

5. Frost & Sullivan: Biometrics can be an alternative to conventional authentication technologies in mobiles
https://ww2.frost.com/news/press-releases/frost-sullivan-biometrics-can-be-alternative-conventional-authentication-technologies-mobiles/

6. How consumers lost $158 billion to cyber crime in the past year... and what to do about it
https://www.forbes.com/sites/stevemorgan/2016/01/24/how-consumers-lost-158-billion-to-cyber-crime-in-the-past-year-and-what-to-do-about-it

7. Global video analytics market to triple over the next decade
http://www.homelandsecurityresearch.com/blog/global-video-analytics-market-to-triple-over-the-next-decade/

8. Hacker fakes German minister’s fingerprints using photos of her hands
https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands

9. Better face-recognition software
https://www.technologyreview.com/s/407976/better-face-recognition-software/

10. FTC issues final commission report on protecting consumer privacy
https://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy

11. The digital universe of opportunities
https://www.emc.com/infographics/digital-universe-2014.htm

12. How the Napa earthquake affected Bay Area sleepers
https://jawbone.com/blog/napa-earthquake-effect-on-sleep/

13. Submit clips of road offences to us: Traffic Police
http://www.straitstimes.com/singapore/submit-clips-of-road-offences-to-us-traffic-police

14. The Dark Secret at the Heart of AI
https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/

15. The Resistance
http://www.washingtonpost.com/sf/national/2015/12/26/resistance

16. Uber’s CEO plays with fire
https://www.nytimes.com/2017/04/23/technology/travis-kalanick-pushes-uber-and-himself-to-the-precipice.html

17. Dialogue with PM Lee Hsien Loong at Camp Sequoia
http://www.pmo.gov.sg/newsroom/dialogue-pm-lee-hsien-loong-camp-sequoia

18. Untangling the way to a Smart Nation
http://www.straitstimes.com/singapore/untangling-the-way-to-a-smart-nation

19. Time for government agencies to be citizen-centric in Singapore’s smart nation push
https://www.techgoondu.com/2017/03/29/time-government-agencies-citizen-centric-singapores-smart-nation-push/

\Orchestrating a brighter world NEC

WE MAKE CITIES SAFER

Using technologies to safeguard lives and property

Global Safety Division | Transportation and City Infrastructure Division

■ nec.com/safety ■ safety@gsd.jp.nec.com