The Road to Collaborative Public Safety

In today's digital economy, a variety of new security threats have emerged. We need to evolve from building urban security systems to enhancing collaborative public security. We must keep pace with rapid societal and technological changes, and improve security arrangements for inter-agency collaboration as well as deepen police-public cooperation.
In Abraham Maslow’s hierarchy of needs, safety, food, and water are the most basic needs for human survival. This is especially true for the growing cities of the world.

Safe City constructions are gaining attention not only for the protection of life and property, but also for the promotion of modern governance. The quality of our lives improves as a result.

For example, the implementation of Kenya’s Safe City project is making obvious improvements in public safety and the healthy development of local tourism. Safe City solutions are proven to be effective in ensuring the safety and security at major public events. The 2015 visit of Pope Francis to Nairobi, for instance, resulted in zero casualties or major incidents among the crowd of 300,000 people. Safe City construction in Saudi Arabia has increased the margins for safety and emergency management for the entire country and, in so doing, laid a solid foundation for further social and financial development.

Global economic integration, changes in social organization, and the rapid digital uplift of industries and social media in recent years have resulted in a constant escalation of security threats faced by the world. Criminals are constantly revising their techniques, and are often armed with the very tools that have been built for commercial and social use. Security threats have now extended from the real world to the Internet. As the cost of committing cybercrime decreases, criminals continue to find novel methods for conducting illegal activities. Transnational organized crime is among the latest of challenges to be addressed in modern Safe City operations.

Huawei is committed to building a better, fully connected world, and Safe City solutions are an integral part of this program. In this new world, safety should be as fundamental as air and water, nurturing everyone in every city, supporting the old and weak, and bringing peace and happiness to everyone. Huawei is working with global industry leaders in the security field to create end-to-end public safety solutions using the platforms and solutions provided by new ICT technologies.

The one-stop ICT solutions provided by Huawei in the Safe Market are now deployed in more than 100 cities in over 30 countries and serve more than 400 million people. Guided by our Business-Driven ICT Infrastructure (BDII) program, Huawei is fulfilling the vision of ‘Leading New ICT, Building a Better Connected World.’ Based on a strategy of integrating new technologies and solutions to deliver ICT-enabled cloud platforms, Huawei is working with partners to build an open, cooperative, and mutually beneficial ecosystem. Our goal is to encourage customers to accelerate the digital transformation processes that promote social harmony and economic development.
[Comment]
1  Leading New ICT, Making Cities Safer

[Features]
4  Smarter Cities: Right Concept, Right Methodology
6  New Insights into Smart City Constructions for ICT Enterprises
9  Location is Everything
12 Safe Cities Need Interoperability
14  A New Paradigm for Security Operations

[Special Report]
18 The Road to Collaborative Public Safety
27 Building an Open Platform for Safe Cities

[Focus]
30 An Evolution in Public Safety Networks
34 Integrating Video and Intelligence for Safe Cities
37 Building Smarter Safe Cities with IoT
40 Cloud Data Centers Improve Police Performance
42 Video Cloud for Integration

[Share Economy]
50 AI Turns Science Fiction into Reality
52 Protecting Enchanted Kenya

[Analyst Corner]
54  Big Data for Public Security

Publisher:
ICT Insights Editorial Board,
Huawei Enterprise

Editors:
Catherine Du  Jeff Peng
Andy Xu  Loren Luo
Caroline Jin  Anilka Zhang
Jing Chen  Sarah Amsar
John North  Pauline Zhang
Sarah Lai  David Lardi
Kaela Jo Ormsby  Gary Taylor
Carolyn Austin

Publisher:
ICT Insights Editorial Board,
Huawei Enterprise

Editors:
Catherine Du  Jeff Peng
Andy Xu  Loren Luo
Caroline Jin  Anilka Zhang
Jing Chen  Sarah Amsar
John North  Pauline Zhang
Sarah Lai  David Lardi
Kaela Jo Ormsby  Gary Taylor
Carolyn Austin
Smart Cities: Right Concept, Right Methodology

By Chen Hongyi, Managing Director, Health & Public Service, Accenture Greater China

Smarter Cities are a significant milestone in the history of metropolitan populations. Multi-faceted Smart City projects are driving substantial changes in production models, city management, and people’s lives. More government agencies, enterprises, social organizations, and citizens worldwide are engaging in Smart City planning and construction. Although most Smart City projects have deployed industry-leading IT infrastructures or added more functionality to legacy eGovernment systems, they have failed to deliver a convenient, cost-effective, and intelligent user experience. One common reason is that project initiators do not approach planning or building Smart Cities from a people-oriented perspective. A second reason is that different government agencies have built information systems that do not connect or share their data. To grow their capabilities, cities must eliminate these information barriers to provide more people-oriented public services. We propose a new methodology for Smart City construction that starts with an in-depth study of people’s needs and evolves into connecting a variety of inter-agency systems and components that enable the development of innovative products.

Meeting People’s Needs

Smart City users are people. So, the question is: How do we conduct such an in-depth study? To answer this, let’s consider sightseeing tours that are provided by many government agencies. From a citizen’s perspective, the process of organizing sightseeing tours must include the following:

• Access to promotional materials
• Ability to make a reservation
• Engagement
• Interaction
• Use of resources

If key resources are missing from the tour, the ‘citizens as customers’ may lose interest in the tour service because of unmet needs. People’s Smart City needs can be summarized as shown in the figure on the right.

Interconnection

Government agencies have built many large and complex public service systems. Traditionally, these structures have their own governance mechanisms, management processes, physical infrastructures, information systems, and personnel. Each may also work with other systems to offer more advanced ‘cross-agency’ services. Due to continuous innovations in new technologies and services, people want to obtain services at a single ‘window’ rather than at different facilities located throughout a city. Fortunately, new ICT advances have made cost-effective, reliable ‘system interconnection’ a reality. The top priority of Smart City projects is the comprehensive internal digitization of each system and the automation, configuration, and modularizing of service functions to build a solid foundation for the integration of innovative, city-wide services.

Cross-Border Innovation

Continuing with the sightseeing tour example, people can obtain tour information by query, reservation, consultation, and even ‘push messages’ from government agencies. Because the tour service information provided by these agencies has come from disparate sources of information, tourists may have difficulty obtaining a complete picture of the available tour packages. After acquiring tour information, visitors must switch to another system for resource reservation and transport services, which can be a complex and time-consuming procedure. To better meet personalized needs, service providers must implement a comprehensive ‘information connection.’ A Smart City system must connect a variety of resources to offer suggestions that cover the entire process of activities. Using ‘cross-agency connections,’ city managers can develop innovative service capabilities that cannot be supplied by a single system.

China’s President Xi Jinping has called for a people-oriented approach to planning and building Chinese government services using advanced information technologies to modernize the country’s governance capabilities. One effective method to develop such an eGovernment platform is to build integrated online service solutions that create a national information sharing resource to help eliminate information barriers and facilitate decision-making.

When analyzing customer needs, we can draw ‘profiles’ that help us develop high-quality, people-oriented services. >>
New Insights into ‘Smart City’ Constructions for ICT Enterprises

By Carol Liao, Senior Partner and Managing Director and Wu Zhizhong, Project Manager, Boston Consulting Group

Safe City constructions combine human resources, physical facilities, and computer technologies to provide solutions that detect, analyze, and integrate the key information of a city’s core operating systems. These solutions contribute to advances in the ‘Smart City,’ a general concept that covers nearly all fields of city development.

The principal goal of Smart Cities is to improve the quality of citizens’ lives and enhance environmental protection, public security, city services, and commerce. To have a more objective understanding of the concept, Information and Communications Technology (ICT) enterprises must break it down. The Boston Consulting Group (BCG) believes that Smart Cities consist of the following five parts.

- **Smart Energy**: Smart Grid and demand-response energy systems, new energy vehicle infrastructure, and distributed-generation integration systems
- **Smart Transport**: Intelligent transportation, congestion solution and tolling systems, smart parking, and intelligent public transport systems
- **Smart Water & Waste**: Intelligent water distribution network and pollution monitoring systems
- **Smart Social & Safe City**: Safety and security systems based on smart monitoring, eGovernment, and remote social insurance systems
- **Smart Buildings**: Building and energy management systems and smart homes

**Smart City Construction Schemes**

Developed and developing countries have different goals and decision-making systems during the constructions of Safe Cities. BCG classifies current Smart City constructions into the following schemes based on such differences:

- **Brownfield Scheme**: Most developed countries are adopting the Brownfield scheme for applying ICT technologies to improve the intelligence of city infrastructure and associated core systems. The ultimate goal is environmental protection and long-term and sustainable city development. Decision makers include the mayor and senior municipal government officials. Central and regional governments provide overall High-Level Designs (HLDs) and make decisions on key issues only. Therefore, the construction scope and progress are deeply affected by the opposition of stakeholders or related laws and regulations.
- **Greenfield Scheme**: The Greenfield scheme is the preferred choice among most developing countries. It focuses on the satellite cities in core economic areas and results in large-scale development starting from scratch. For countries adopting this scheme, regional and city development plans are more important than the application of ICT technologies. The ultimate goal is to boost the economy of a city by leveraging certain benefits of constructing each Smart City, such as investment growth, land value increases, and additional services. Central and other higher-level governments make the decisions. Smart City installations are generally part of an overall national or regional development plan, which serves to guarantee their implementation. The scope and progress of the physical attributes seldom change, even when there are objections.

**Further Investment brings additional decision-making power and higher risks.** Some projects require more decision making power, while others require lower risks. ICT enterprises must make choices based on actual conditions. The investment percentage of private companies will rise because of increasing government debts and clearer monetization schemes. This requires a more comprehensive project and financial strategy for future cooperation between companies and governments.
**Insufficient Investment Impedes Growth**

Cause: Local governments are reluctant to continue the usual practice of debt financing. For ICT enterprises, financing is an increasingly large challenge.

Insight: To obtain sufficient capital, ICT enterprises must improve their own financing capabilities and enhance cooperation with other financing entities.

**Limited Vertical Integration Obscures**

Cause: ICT enterprises have yet to acquire a clear monetization scheme.

Insight: ICT enterprises need to identify more profit points and establish a clear path to monetization.

**General Lack of Business Cases Prevents**

Cause: Current cases have their own characteristics that cannot be generalized into standard business schemes.

Insight: ICT enterprises need to enhance one-stop service capabilities, locate past points, obtain city construction requirements, and develop unified solutions that can be applied across the board.

**Location is Everything**

By Andy Rooke, EENA Member, Vice President, British-APCO, Director, ShadowFocus Consultancy Ltd.

"Police Emergency. What is your location?"

"I've crashed my car into a ditch and my boyfriend is not moving. Please help us!"

"I've not only spent my 30 plus year career trying to find and help victims of car accidents or crime but also helping emergency services improve their technology for communicating with each other by voice and data to speed their response times."

Our motto for an effective emergency services response is: 'Right Response, Right Place, and Right Time.'

This saying is as true now as when first coined in the 1990s. The major problem is that most call-takers and dispatch systems are not yet capable of identifying the location of 911/112 calls from mobile handsets — and, in many countries, the majority of calls are now coming from mobile devices.

The public also has a role to play because very few people are aware of their surroundings, especially during an emergency. When driving, we tend to follow our satellite navigation units until the devices say: "You have reached your destination." When emergencies occur, people must quickly determine their location; and in the midst of a crisis, we are very often incorrect.

Mobile network providers can give only an ellipse location to the emergency call-taker. Locations are derived from mobile phone mains and signal strength.

Andy Rooke, EENA Member, Vice President, British-APCO, Director, ShadowFocus Consultancy Ltd.
features

Key Technologies

Automatically, key technologies to be introduced over the next two years are designed to fundamentally change how emergency service agencies receive, process, and respond to emergency calls.

eCall

eCall will come to Europe in 2018 and, by law, compliant devices will be installed for free in every new car and light truck. If an accident occurs, the on-vehicle equipment will dial the 112 European emergency number and send a data message with exact GPS coordinates, direction of travel, pean emergency number and send a data message the on-vehicle equipment will dial the 112 European emergency number and send a data message.

Vehicle Location (A VL) further boosts this intelligence for dispatchers and first responders.

Analyzing and Review

Post-incident management is as important as the original response but is often overlooked. With a complete and accurate debriefing of the sources will have been provided over an extended period, the incident, can then begin to build a more complete and accurate picture of the incident with live video feeds to the command center. The dispatcher, who has tactical command of the incident, can then begin to build a more complete picture of the incident, and allocate additional resources where necessary.

Vehicle Location (A VL) further boosts this intelligence for dispatchers and first responders.
Safe Cities Need Interoperability

By Per Bjorkdahl, Chairman, ONVIF Steering Committee

The integration of component parts to create a single interoperable platform is one of the great challenges for every Safe City deployment. The most common scenario is that municipalities have multiple legacy systems from different manufacturers, each with proprietary interfaces. To interconnect these systems, cities will often employ a “build-once-maintain forever” approach that creates technical complexity and an ongoing, uncapped expense.

Enter Standards

ONVIF—launched in 2008 as the Open Network Video Interface Forum—is an industry alliance that offers standardized interface specifications for IP-based video security and access control systems that are at the heart of modern Safe City solutions. Specifically designed to overcome the challenges in multi-vendor environments, ONVIF’s common interfaces facilitate communication between equipment from different manufacturers and foster an interoperable environment where system components can be used interchangeably.

Essential for the effective integration of the wide variety of client devices used by the physical security industry, recently released ONVIF specifications include ‘Profile S’ for video streaming and ‘Profile G’ for video storage and playback. The current release candidate, ‘Profile Q’ for automated device discovery and configuration, is scheduled for final release in July 2016.

In Safe City scenarios, much of the video ingested by security systems is used to conduct post-event forensic investigations that are critical to working with its members to develop an all-encompassing, multi-variant standard that will satisfy the core elements for video surveillance, access control, and every other essential operation relevant to the functionality of Safe City command centers.

ONVIF Members Deploy Safe City Solutions

In 2014, Meyertech, a British technology company and Video Management Software (VMS) developer, helped York, England deploy a Safe City solution for the city’s public spaces and transportation system. Using their ONVIF-compliant video and information management software, Meyertech integrated new equipment with legacy systems for the York Travel and Control Centre command center. The control room has been configured to monitor over 150 cameras from multiple manufacturers that are installed throughout the city. Government officials reported an immediate reduction in the rate of crime due, in part, to the Meyertech VMS platform.

Huawei, a global leader in the Safe City market, has deployed Safe City solutions in over 200 cities throughout Africa, Europe, the Middle East, and Asia-Pacific. One of many examples for the utility of ONVIF’s interface standards was a Shanghai project, under the auspices of a Chinese government Ministry of Public Security initiative, where the Huawei VMS was used to integrate old and new camera equipment from Sony, Dahua, Hikvision, and others.

A Multi-discipline Physical Security Standard

Expect physical security to play a substantial role in the evolving Internet of Things (IoT). ONVIF envisions that all-endpoint devices in the universe of physical security will present an identical interface for the purpose of achieving interoperability. To this end, ONVIF is dedicated to working with its members to develop an all-encompassing, multi-variant standard that will satisfy the core elements for video surveillance, access control, and every other essential operation relevant to the functionality of Safe City command centers.

Technology experts, including the Institute of Electrical and Electronics Engineers (IEEE), are working on a set of global IoT standards that some predict will be in place by the end of 2016. If such IoT standards are developed, we at ONVIF expect that their influence on Safe City deployments will be profound and far-reaching for safety and security worldwide.

Safe Cities Need Interoperability

By Per Bjorkdahl, Chairman, ONVIF Steering Committee

1. The integration of component parts to create a single interoperable platform is one of the great challenges for every Safe City deployment.
2. The most common scenario is that municipalities have multiple legacy systems from different manufacturers, each with proprietary interfaces.
3. To interconnect these systems, cities will often employ a “build-once-maintain forever” approach that creates technical complexity and an ongoing, uncapped expense.
4. ONVIF—launched in 2008 as the Open Network Video Interface Forum—is an industry alliance that offers standardized interface specifications for IP-based video security and access control systems that are at the heart of modern Safe City solutions.
5. Specifically designed to overcome the challenges in multi-vendor environments, ONVIF’s common interfaces facilitate communication between equipment from different manufacturers and foster an interoperable environment where system components can be used interchangeably.
6. Essential for the effective integration of the wide variety of client devices used by the physical security industry, recently released ONVIF specifications include ‘Profile S’ for video streaming and ‘Profile G’ for video storage and playback.
7. The current release candidate, ‘Profile Q’ for automated device discovery and configuration, is scheduled for final release in July 2016.
8. In Safe City scenarios, much of the video ingested by security systems is used to conduct post-event forensic investigations.
9. Meyertech, a British technology company and Video Management Software (VMS) developer, helped York, England deploy a Safe City solution for the city’s public spaces and transportation system.
10. Using their ONVIF-compliant video and information management software, Meyertech integrated new equipment with legacy systems for the York Travel and Control Centre command center.
11. The control room has been configured to monitor over 150 cameras from multiple manufacturers that are installed throughout the city.
12. Government officials reported an immediate reduction in the rate of crime due, in part, to the Meyertech VMS platform.
13. Huawei, a global leader in the Safe City market, has deployed Safe City solutions in over 200 cities throughout Africa, Europe, the Middle East, and Asia-Pacific. One of many examples for the utility of ONVIF’s interface standards was a Shanghai project, under the auspices of a Chinese government Ministry of Public Security initiative.
14. Technology experts, including the Institute of Electrical and Electronics Engineers (IEEE), are working on a set of global IoT standards that some predict will be in place by the end of 2016.
By Dr. Amanat Hussain, Chief Operating Officer, BGS Ltd.

The policing and security landscape is increasingly complex, unpredictable, and interconnected. Police and security organizations are required to operate in turbulent environments with unexpected events, uncertainty and lack of control, complex decision making, group interdependencies, and growing demands for efficiency and high performance across work boundaries that are often unclear.

Policing with this kind of complexity requires enhanced capabilities for counter-extremism and protective security, including tightened controls at ports, airports, and borders. A holistic approach is necessary to address a long list of issues:

- Effective policing in complex environments.
- To facilitate a professional response to security incidents through more preventative and mission-focused deployment of resources.
- Greater community engagement to develop trust and a community services culture within security organizations.
- Improved management of security targets and intelligence agencies, protection units, local authorities, private sector organizations, and community groups.
- Provision for the vulnerability in society.
- Improved service delivery to the public and a timely, effective response.
- Integrated information and intelligence to ensure that decisions follow established priorities and that the most appropriate resources are allocated in response to scalable for assistance and emerging intelligence.
- Efficient and effective policing to deliver the most value for the investment.

Safer City Initiatives

Policing systems require greater integration to deliver more sophisticated and effective public services. Solely needed are programs that modernize police systems with more flexible resources for today’s dynamic and complex policing environment. ICT infrastructure with multi-channel demand management capabilities, policies, and processes must be aligned with staff capabilities to ensure support for converging operational requirements as they evolve. In short, effective policing systems need:

- Integrated awareness of policing and security demands and improved preparation for police to respond more effectively to these demands.
- Better data communication, voice communication, and coordination across security and partner agencies.
- Greater community engagement to develop trust and a community services culture within security organizations.
- Integrated information and intelligence to ensure that decisions follow established priorities and that the most appropriate resources are allocated in response to scalable for assistance and emerging intelligence.
- Efficient and effective policing to deliver the most value for the investment.

The Safe City C3iStar solution provides a converged multi-agency platform for police and other emergency services, traffic patrol, anti-terror units, intelligence agencies, protection units, local authorities, private sector organizations, and community groups. This solution builds an integrated network of sensors and communication platforms that enable all public safety, law enforcement, and related agencies to access context-specific intelligence for managing real-time events and providing seamless service delivery to the public. The platform also enables a networked operating model that connects all organizational components and assets and, where possible, relevant components of partner agencies. The C3iStar solution also integrates knowledge with decision support tools and is a system of services and deployments within a wider command and control environment.

The C3iStar platform integrates knowledge with decision support tools and is a system of services and deployments within a wider command and control environment. The converged platform addresses both the demand management and resource management functions within policing and security organizations. Central to its operation is the Decision Support and Intervention Platform, which is underpinned by context-specific intelligence. This intelligence is
Police mobility requirements, however, are not just about technologies; they are also about people and organizations. They need to be aligned with new operating models and processes that transform the organization, along with clearly defined roles and responsibilities, including the authority to make discretionary decisions that maximize effectiveness.

● Operations Alignment
There is little value in having cutting-edge technology if the roles, performance measures, and employee reward and promotion systems encourage the wrong behaviors. Leadership teams need to be aligned with the transformation and engaged in driving behaviors and practices that mobilize staff to embrace new ways of working. Alignment between the organizational and individual performance management systems is essential for having individual police officers and staff members see how their performance goals fit in with the broader targets of the organization. This ensures that the right outcomes and behaviors are recognized and rewarded.

● Concept of Operations
Operations models should be reviewed and updated to optimize cross-agency coordination, communication, and effectiveness in public safety and emergency services. With Safe City infrastructure, policing operations can progress to become more proactive and prevention-based via enhanced access to information and intelligence.

For too often technology is used to perpetuate outdated operational models that result in few actual benefits being realized from a new investment. The effect of digitalization is the dynamic management of looking, listening, and attributing against threats, risks, and events, and continually collects information to monitor and evaluate strategy, tactics, and performance outcomes to identify the gaps between projected and actual results.

● Building Leadership
Leadership at all levels of each organization must commit to the implementation of Safe City best practices through both words and actions. The ability to change within a changing environment is problematic if what is considered "leadership" is exercised only by the most senior officers and staff. The development of leadership skills is beneficial for everyone within the organization because staff members empowered to think outside the box and act creatively will most often deliver the best results.

Maintaining leadership support involves making sense of each situation and providing explanations that are meaningful to operations personnel and stakeholders within the police force. The end result promotes a deeper understanding of the underlying reasons for change and makes appropriate actions. Solid leadership enables large organizations to move forward with a shared vision and commitment to meet every challenge with the highest levels of professionalism and integrity.

Enhanced operational awareness allows officers and staff to see and understand current, emerging, and potential security needs as if looking through a threat-risk prevention and reduction ‘lens.’ The system tracks all available and potentially available resources by location, skills, capability, and availability. This allows the police force to allocate and deploy people and other resources intelligently, according to set guidelines for potential risks and outcome priorities. The Safe City CJIS platform ensures that officers have the context and situational awareness necessary to manage events as they unfold. For example, an officer dispatched to a domestic disturbance may be automatically alerted or reminded that a suspect lives nearby and is on bail for a serious offense. This scenario would permit the officer or supervisor to intelligently update with information held in police data systems about previous activities, including vulnerable individuals or any other potential threats, such as domestic abusers, sex offenders, andgadores.

A firearms license.

Police frequency.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.

A firearms license.
Digital Economy or Digital Disruption?

We are already in the age of digital economy. Leveraging technologies, people are connecting to people directly (even things to things directly), facilitating crowd-sourcing, increasing efficiencies of traditional processes, and even creating new business models such as Uber, Airbnb, Alibaba, Facebook, WeChat, and many others. While these successful new business models are celebrating the Digital Economy, traditional companies, from taxi to hotel to telco, see this as Digital Disruption. Industries which are not already transforming themselves will soon be disrupted by this Digital Economy.

Unfortunately, the bad guys are also transforming themselves; maximizing the return on their evil doings through the use of technologies driving this Digital Economy: Social, Mobile, Cloud, and Big Data! We see some extremist groups using such technologies aggressively to radicalize people far away online, to recruit armed men, to seek finance, and even to collect intelligence. These groups are the Digital Economy disruptors of the old extremism school.

Likewise, people with ill intent are organizing public security threats through the use of technology. Social media is a scary means of spreading rumors, and together with the pervasiveness of mobile devices, it is very easy to organize a flash mob. Thousands of people with group psychology kicking in can turn a peaceful movement to a violent event quickly, resulting in injuries and even deaths. During the 2011 England security incidents, there was even a mobile App, Sukey, with the specific goal of frustrating police operations against the rioters.

A daily concern to all is physical crime, ranging from homicide to robbery to burglary to theft to many other street crimes. Increasingly crimes are being facilitated through digital technologies too. In 2014, about 42% of vehicles stolen in London were not by traditional brute force, but through digital hacking! Singapore saw in 2015 a decrease in traditional crimes, but there was a surge of online scams, resulting in a 4% rise in overall crime! Such a trend is not unique, particularly among developed countries.

The use of digital technologies is also giving rise to many cases of cyber attacks, especially that against critical infrastructures globally; such as the Gundremmingen nuclear power plant in Germany that was infected with computer viruses.

From acts of extremism to public security threats to physical crimes to cyber attacks, the bad guys are leveraging the Digital Economy. These are not the usual form of cyber-crime such as web defacement and theft of information, they are cyber-facilitated extremism and organized crime. As witnessed in the changing face of crime in safe cities such as Singapore, the sense of safety fostered by conventional policing for street crimes is being disrupted; more needs to be done to fight such cyber-facilitated extremism and crimes. Even public safety agencies have to catch up with the Digital Economy, and avoid being at the receiving end of disruptors.

At the 13th UN Congress on Crime Prevention and Criminal Justice, UN Secretary-General Ban Ki-moon remarked that, “Like never before, terrorists and criminals around the world are coming together and feeding off each other. They are funding terror through criminal networks and growing rich through the suffering of entire populations.”

This is why we need to form a network of good guys to fight the network of bad guys. At the same time, the good guys also have to work together to deal with accidents and natural disasters. While not all accidents can be avoided, more can be done in regulatory control, enforcement and cross-agency coordination. Similarly, for natural disasters, efforts can be increased to identify threats, detect and provide...
early warning, thereby reducing the impact, and aiding the recovery process.

The Digital Economy is also changing people’s behavior. The “MeFirst” generation is likely to Tweet, Facebook, or WeChat a photograph of an accident or crime before he or she calls the emergency number. But such behavior is not exactly bad; it provided the authority with loads of valuable photographic and video during the Boston Marathon in 2013, a great example of “It Takes a Network to Fight a Network” which will be elaborated later.

Safe City

Safe City is against conventional threats or threats arising from digital technologies. Safe City implementation remains critical globally. According to IHS Technology, video surveillance, Long-Term Evolution (LTE), and command and control solutions are the backbone of a Safe City. IHS estimated the Safe City market was worth $5.6 billion in 2015, and reaching $8.5 billion by 2019. The three key aims of Safe City solutions are: Well public safety organizations in collecting, sharing and analyzing data more effectively to provide a common operational picture and raising situational awareness.

Be it against conventional threats or that arising from digital technologies, Safe City implementation remains critical globally. According to IHS Technology, video surveillance, Long-Term Evolution (LTE), and command and control solutions are the backbone of a Safe City. IHS estimated the Safe City market was worth $5.6 billion in 2015, and reaching $8.5 billion by 2019. The three key aims of Safe City solutions are: Well public safety organizations in collecting, sharing and analyzing data more effectively to provide a common operational picture and raising situational awareness.

To implement reliable and all-coverage security measures to detect threats and situations as they emerge.

Aid public safety organizations in collecting, sharing and analyzing data more effectively to provide a common operational picture and raising situational awareness.

To implement reliable and all-coverage security measures to detect threats and situations as they emerge.

Public Safety

Public Safety refers to the public safety, from street crimes to extremism to accidents to disasters, will always be a challenge to all cities. While a Safe City implementation is a core capability of modern policing and emergency services, it currently mainly covers detection, sense-making to quick solving of the case. The Video Content Management also comes with more than 20 intelligent analytics including entity recognition, crowd counting, and virtual tripwires. The tiered Video Cloud Storage provides cost-efficient archival of video footages, at both remote sites and centralized location. Huawei offers high definition IP Cameras that come with their own power supply too.

Public Warning

Examples of Public Warning include the island-wide public warning system in Singapore, and the Japan’s earthquake warning through their Social networking. Such voice, video, and data can then be routed to Social networking sites. As mentioned earlier, Huawei’s Intelligent Communication Platform can ingest data from IoT and Social networking. Such behavior is not exactly bad; it provided the authority with loads of valuable photographs and videos during the Boston Marathon in 2013, a great example of “It Takes a Network to Fight a Network” which will be elaborated later.

Public Safety

Public Safety refers to the public safety, from street crimes to extremism to accidents to disasters, will always be a challenge to all cities. While a Safe City implementation is a core capability of modern policing and emergency services, it currently mainly covers detection, sense-making to quick solving of the case. The Video Content Management also comes with more than 20 intelligent analytics including entity recognition, crowd counting, and virtual tripwires. The tiered Video Cloud Storage provides cost-efficient archival of video footages, at both remote sites and centralized location. Huawei offers high definition IP Cameras that come with their own power supply too.
It Takes a Network to Fight a Network

To achieve Collaborative Public Safety, we need to consider the four pillars behind the Network of good guys:

• Inter-Agency Collaboration. Extremism, criminals, and even pandemics strike across boundaries and sovereign borders. All public safety agencies in a country, and across countries, have to collaborate to fight such threats. Collaboration includes sharing of information and best practices, interoperability of communication methods, and coordinated joint actions.

• Public-Private Partnership. Public safety agencies have to partner the community, businesses, non-profit organizations, and academia to prevent, detect, respond, and recover from threats. The bad guys are networking and collaborating, so must the good guys!

• Partners Ecosystem. Cyber-facilitated threats in this age of Digital Economy are very much fueled by technologies. Likewise, an ecosystem of technologies is needed to enable the collaboration and partnership mentioned above.

• Leading New ICT. Technological solutions need to run on a secured and robust platform, supporting data, voice, video, and even IoT. With its globally proven information, communication, and networking technologies, Huawei’s Leading New ICT is the fourth pillar behind this Network of good guys.

Currently, Safe City implementation remains the foundation for a good Public Safety execution. Even while basic elements of a Safe City are being implemented, it is imperative for governments to start working towards Collaborative Public Safety.

Prevention is better than cure. As articulated by Sir Robert Peel in 1829, the absence of crime and disorder is the real test for police efficiency. One cannot prevent if one cannot even identify the threats. Predictive policing, or PredPol, involves analysis of data to predict the next crime, with the objective of preventing it. With potential threats identified, governments have to enact regulations, require licensing, and carry our enforcements. For example, the US Department of Transportation has to manage more than 300,000 companies that ship more than one million daily shipments of HAZMAT (hazardous materials). The Department uses a risk-based data-driven approach to identify and target high-risk companies, and improve safety through risk-based enforcement and prioritizing inspection activities. Other forms of licensing and enforcement include fire safety inspection, building code, alcohol control, traffic enforcement, etc. Even Border Protection is a form of licensing and enforcement to prevent threats. Border Protection includes visa application & screening, passenger & cargo risk management (e.g. US Customs and Border Protection’s Automated Targeting System), and entry/exit systems.

Despite best efforts, some threats just cannot be prevented. This is why simulations and forecasts are needed to reduce the loss of life and property. After the 2004 Asian Tsunami, the Pacific Disaster Center (PDC) helped the Thai Government to build a National Disaster Warning Center using PDC’s DisasterAWARE solution that simulates and forecasts disasters by analyzing data including those from IoT.

Threats when actualized will lead to the Detection and Response phases (Safe City), which were described in the previous section of this paper. In line with the full definition of Public Safety, governments are expected to minimize the disruption to life. This is when we enter...
implementations with no sharing of information; going against the principle of inter-agency collaboration. Furthermore, individual implementation requires separate infrastructure, from the network to storage to server to database to middleware to device. This is clearly a waste of resources.

Therefore, governments need a roadmap for the rolling out of the different vertical applications on a common scalable Policing Cloud platform, usually private due to security requirements of public safety. Such common platforms running different applications not only can better facilitate information sharing, but also dynamically allocate the appropriate computing power to different applications. For example, after a disaster, the victim identification system can be allocated more computing power since thousands of people will be using this system to check on their loved ones.

To ensure more choices of Independent Software Vendors (ISVs) for the different vertical applications, the cloud platform has to be

During major incidents, there will be a need for a Whole-of-Government Command Center at the national level, which is also a great platform for intelligence fusion and analysis.

The Collaborative Public Safety concept is applicable to all manner and scale of threats. During major incidents, there will be a need for a Whole-of-Government Command Center at the national level, which is also a great platform for intelligence fusion and analysis.

It is unfortunate that even within the investigation function, there are different specialists in a single law enforcement agency. This has often resulted in different stove-piped systems, creating inconvenience to the victims, witnesses, and even law enforcement officers. Finland Police is implementing the VITJA project to address such issues.

Another example is in the City of Qiqihar in China. With a population of 5.4 million, the 5,000 private taxis are equipped with cameras that can transmit video real-time through eLTE wireless network. In the event of an incident or crime, the police control room can access such video real-time from taxis in the vicinity. This collaboration has already helped solve a number of crimes.

Policing Cloud and Big Data

While the backbone of a Safe City comprises video surveillance, LTE, and command and control solutions, the backbone of the wider Collaborative Public Safety is the tens, if not hundreds, of vertical applications spanning Prevention, Detection, Response, Recovery, and even Social Engagement. Unfortunately, these vertical applications usually fall under the purview of different departments, resulting in separate stand-alone implementations with no sharing of information; going against the principle of inter-agency collaboration. Furthermore, individual implementation requires separate infrastructure, from the network to storage to server to database to middleware to device. This is clearly a waste of resources.

Therefore, governments need a roadmap for the rolling out of the different vertical applications on a common scalable Policing Cloud platform, usually private due to security requirements of public safety.

As part of the investigation process, a criminal intelligence system is needed to identify those who are injured and their whereabouts, as well as those who have died. Families and friends of victims may pose a secondary public safety problem if they do not receive timely information about their loved ones.

The Collaborative Public Safety concept is applicable to all manner and scale of threats. During major incidents, there will be a need for a Whole-of-Government Command Center at the national level, which is also a great platform for intelligence fusion and analysis.

The Fort McMurray wildfire in Canada in May 2016 was massive. More than 88,000 people were displaced from their homes. While the fire itself was a major incident; the poor management of survivors can lead to another major event, including epidemics due to poor water and food supplies, sanitation, and looting as had happened after Hurricane Katrina struck New Orleans. Usually neglected, a good Public Safety program needs to include assistance for survivors.

Similarly, a victim identification system is needed to identify those who are injured and their whereabouts, as well as those who have died. Families and friends of victims may pose a secondary public safety problem if they do not receive timely information about their loved ones. As part of the investigation process, a criminal intelligence system is needed to establish links between people, objects, locations, and events, and to narrow down the suspects. With the investigation completed, an inquiry or court hearing is needed to close the loop. Rehabilitation, including punishment and improvement, aims to prevent the recurrence of such threats. The lessons learnt provide inputs back to the Prevention phase.

Collaborative Public Safety requires processes and technologies for Social Engagement, Crowd Sourcing and Public Communication. An interesting example is the Singapore Civil Defence Force’s (SCDF) myResponder. People trained in Cardiopulmonary Resuscitation (CPR) can register as volunteers and use the myResponder mobile App. When there is an incident of heart attack, the SCDF control room will dispatch an ambulance, and at the same time send a message to those myRe- sponder volunteers in the vicinity. The App will also alert the volun- teers of the nearest Automated External Defibrillator (AED). Several lives have already been saved through such “crowd-dispatch.”

Another example is in the City of Qiqihar in China. With a population of 5.4 million, the 5,000 private taxis are equipped with cameras that can transmit video real-time through eLTE wireless network. In the event of an incident or crime, the police control room can access such video real-time from taxis in the vicinity. This collaboration has already helped solve a number of crimes.

Policing Cloud and Big Data

While the backbone of a Safe City comprises video surveillance, LTE, and command and control solutions, the backbone of the wider Collaborative Public Safety is the tens, if not hundreds, of vertical applications spanning Prevention, Detection, Response, Recovery, and even Social Engagement.

Unfortunately, these vertical applications usually fall under the purview of different departments, resulting in separate stand-alone implementations with no sharing of information; going against the principle of inter-agency collaboration. Furthermore, individual implementation requires separate infrastructure, from the network to storage to server to database to middleware to device. This is clearly a waste of resources.

Therefore, governments need a roadmap for the rolling out of the different vertical applications on a common scalable Policing Cloud platform, usually private due to security requirements of public safety.

As part of the investigation process, a criminal intelligence system is needed to establish links between people, objects, locations, and events, and to narrow down the suspects. With the investigation completed, an inquiry or court hearing is needed to close the loop. Rehabilitation, including punishment and improvement, aims to prevent the recurrence of such threats. The lessons learnt provide inputs back to the Prevention phase.

Collaborative Public Safety requires processes and technologies for Social Engagement, Crowd Sourcing and Public Communication. An interesting example is the Singapore Civil Defence Force’s (SCDF) myResponder. People trained in Cardiopulmonary Resuscitation (CPR) can register as volunteers and use the myResponder mobile App. When there is an incident of heart attack, the SCDF control room will dispatch an ambulance, and at the same time send a message to those myRe- sponder volunteers in the vicinity. The App will also alert the volun- teers of the nearest Automated External Defibrillator (AED). Several lives have already been saved through such “crowd-dispatch.”

Another example is in the City of Qiqihar in China. With a population of 5.4 million, the 5,000 private taxis are equipped with cameras that can transmit video real-time through eLTE wireless network. In the event of an incident or crime, the police control room can access such video real-time from taxis in the vicinity. This collaboration has already helped solve a number of crimes.

Policing Cloud and Big Data

While the backbone of a Safe City comprises video surveillance, LTE, and command and control solutions, the backbone of the wider Collaborative Public Safety is the tens, if not hundreds, of vertical applications spanning Prevention, Detection, Response, Recovery, and even Social Engagement.

Unfortunately, these vertical applications usually fall under the purview of different departments, resulting in separate stand-alone implementations with no sharing of information; going against the principle of inter-agency collaboration. Furthermore, individual implementation requires separate infrastructure, from the network to storage to server to database to middleware to device. This is clearly a waste of resources.

Therefore, governments need a roadmap for the rolling out of the different vertical applications on a common scalable Policing Cloud platform, usually private due to security requirements of public safety.

As part of the investigation process, a criminal intelligence system is needed to establish links between people, objects, locations, and events, and to narrow down the suspects. With the investigation completed, an inquiry or court hearing is needed to close the loop. Rehabilitation, including punishment and improvement, aims to prevent the recurrence of such threats. The lessons learnt provide inputs back to the Prevention phase.

Collaborative Public Safety requires processes and technologies for Social Engagement, Crowd Sourcing and Public Communication. An interesting example is the Singapore Civil Defence Force’s (SCDF) myResponder. People trained in Cardiopulmonary Resuscitation (CPR) can register as volunteers and use the myResponder mobile App. When there is an incident of heart attack, the SCDF control room will dispatch an ambulance, and at the same time send a message to those myRe- sponder volunteers in the vicinity. The App will also alert the volun- teers of the nearest Automated External Defibrillator (AED). Several lives have already been saved through such “crowd-dispatch.”

Another example is in the City of Qiqihar in China. With a population of 5.4 million, the 5,000 private taxis are equipped with cameras that can transmit video real-time through eLTE wireless network. In the event of an incident or crime, the police control room can access such video real-time from taxis in the vicinity. This collaboration has already helped solve a number of crimes.

Policing Cloud and Big Data

While the backbone of a Safe City comprises video surveillance, LTE, and command and control solutions, the backbone of the wider Collaborative Public Safety is the tens, if not hundreds, of vertical applications spanning Prevention, Detection, Response, Recovery, and even Social Engagement.

Unfortunately, these vertical applications usually fall under the purview of different departments, resulting in separate stand-alone implementations with no sharing of information; going against the principle of inter-agency collaboration. Furthermore, individual implementation requires separate infrastructure, from the network to storage to server to database to middleware to device. This is clearly a waste of resources.

Therefore, governments need a roadmap for the rolling out of the different vertical applications on a common scalable Policing Cloud platform, usually private due to security requirements of public safety.

As part of the investigation process, a criminal intelligence system is needed to establish links between people, objects, locations, and events, and to narrow down the suspects. With the investigation completed, an inquiry or court hearing is needed to close the loop. Rehabilitation, including punishment and improvement, aims to prevent the recurrence of such threats. The lessons learnt provide inputs back to the Prevention phase.

Collaborative Public Safety requires processes and technologies for Social Engagement, Crowd Sourcing and Public Communication. An interesting example is the Singapore Civil Defence Force’s (SCDF) myResponder. People trained in Cardiopulmonary Resuscitation (CPR) can register as volunteers and use the myResponder mobile App. When there is an incident of heart attack, the SCDF control room will dispatch an ambulance, and at the same time send a message to those myRe- sponder volunteers in the vicinity. The App will also alert the volun- teers of the nearest Automated External Defibrillator (AED). Several lives have already been saved through such “crowd-dispatch.”

Another example is in the City of Qiqihar in China. With a population of 5.4 million, the 5,000 private taxis are equipped with cameras that can transmit video real-time through eLTE wireless network. In the event of an incident or crime, the police control room can access such video real-time from taxis in the vicinity. This collaboration has already helped solve a number of crimes.
Building an Open Platform for Safe Cities

By Bai Jianhua, General Manager, Government Solutions, Enterprise Business Group, Huawei Technologies Co., Ltd.

S

tolving complex crimes in heavily populated urban centers requires advanced security technologies and an adequate police force. Public security agencies are now exploring Safe City platforms that use the latest security technologies to improve efficiency, high-tech crime detection, and crime prevention, and expand police services on demand.

Open, Decoupled, and Modularized

Most Safe City systems today are highly customized solutions involving multiple vendors. Service upgrades on such legacy systems are costly and time consuming. An additional complication is vendor lock-in. Although the old system may feature converged elements (terminals, networks, services), what it lacks is an open, decoupled, and modularized platform.

By Bai Jianhua, General Manager, Government Solutions, Enterprise Business Group, Huawei Technologies Co., Ltd.

An additional issue is the cyberspace domain, as opposed to the physical realm. Traditionally, government departments have their own Command & Control centers. Through communication and collaboration, these separate centers can usually work together to achieve their common mission in upholding public safety.

However, during major incidents, there will be a need for a Whole-of-Government Command Center at the national level, which is also a great platform for intelligence fusion and analysis. For a big city, each area, province, or even major city may have such center. During times of normalcy, each center can be manned by a small team of officers. During a major incident, the Head of State or City will be there to exercise whole-of-government command. Usually the heads of the relevant major government agencies will be there too. Such a center will need to be connected to all the major departmental Command & Control centers.

Summary

The good guys have to embrace the Digital Economy and form a Network to fight against the Network of bad guys, who are already leveraging the technologies behind Digital Economy: Social, Mobile, Cloud, and Big Data. This is the spirit behind Collaborative Public Safety, in respect of technology, requires an OpenStack based Policing Cloud platform.

While Safe City has a backbone of video surveillance, LTE, and Command and Control solutions, Collaborative Public Safety, in respect of technology, requires an OpenStack based Policing Cloud platform to support the many vertical applications that will be rolled out over time. Many of such applications require the use of Big Data and Analytics. The apex of Collaborative Public Safety is the Whole-of-Government Command Center, which may include a NSCOC to oversee the security of the cyberspace.

OpenStack-based Cloud OS: Services feature high compatibility and capability for continuous evolution.

● End-to-End (E2E): System-level solutions, such as power supply, air conditioning, lightning protection, and firefighting, equipment-level solutions, such as network, IT, and security devices; plus unified Network Management System (NMS).

● Data Center (DC): Single cabinet MicroDCs; containerized DCs; modular DCs that support quick installation and smooth expansion; traditional DCs for rack space deployment.

● Resource management and disaster recovery: Unified and resilient, distributed cloud DCs.

● Intelligent Monitoring Platform.

● Video Monitoring Systems (VMS): Support cameras from different vendors and shared access to social video resources. Video resources are stored and shared across locations, departments, and types with a global catalog view. VMSs provide fast, secure, distributed cloud data storage with real-time content viewing of large-scale videos and query response times in seconds.

● Video Content Management (VCM) provides parallel and structured cloud computing. Big Data, and the Internet of Things (IoT), is the foundation of the Huawei Safe City architecture.

The core products and services for the Huawei Safe City solution include:

• FusionSphere: Distributed Cloud Platform

• OpenStack-based Cloud OS: Services feature high compatibility and capability for continuous evolution.

• Video Monitoring Systems (VMS): Support cameras from different vendors and shared access to social video resources. Video resources are stored and shared across locations, departments, and types with a global catalog view. VMSs provide fast, secure, distributed cloud data storage with real-time content viewing of large-scale videos and query response times in seconds.

• Video Content Management (VCM) provides parallel and structured cloud computing. Big Data, and the Internet of Things (IoT), is the foundation of the Huawei Safe City architecture.

The Huawei Safe City solution constructs an open ecosystem with customers and industry partners. >>

Building an Open Platform for Safe Cities

By Bai Jianhua, General Manager, Government Solutions, Enterprise Business Group, Huawei Technologies Co., Ltd.

S

tolving complex crimes in heavily populated urban centers requires advanced security technologies and an adequate police force. Public security agencies are now exploring Safe City platforms that use the latest security technologies to improve efficiency, high-tech crime detection, and crime prevention, and expand police services on demand.

Open, Decoupled, and Modularized

Most Safe City systems today are highly customized solutions involving multiple vendors. Service upgrades on such legacy systems are costly and time consuming. An additional complication is vendor lock-in. Although the old system may feature converged elements (terminals, networks, services), what it lacks is an open, decoupled, and modularized platform.

By Bai Jianhua, General Manager, Government Solutions, Enterprise Business Group, Huawei Technologies Co., Ltd.

An additional issue is the cyberspace domain, as opposed to the physical realm. Traditionally, government departments have their own Com- poster Emergency Response Team (CERT) and/or Security Information & Event Management (SIEM) centers. But with increasing complex- ity and scale of cyber-facilitated extension/crime described above, countries have started to invest in National Cyber Security Operations Center (NSCOC).

NSCOC usually receives data from all the CERT/SEIM centers. The objective is for a country to detect a major attack against any industry by analyzing all these streams of data via Big Data-based Network Behavior Anomaly Detection (NBAD). Examples include Intel’s Cyber Security Bureau and U.S. Cyber Threat Intelligence Integration Center.

While Safe City has a backbone of video surveillance, LTE, and Command and Control solutions, Collaborative Public Safety, in respect of technology, requires an OpenStack based Policing Cloud platform to support the many vertical applications that will be rolled out over time. Many of such applications require the use of Big Data and Analytics. The apex of Collaborative Public Safety is the Whole-of-Government Command Center, which may include a NSCOC to oversee the security of the cyberspace. ●

OpenStack-based Cloud OS: Services feature high compatibility and capability for continuous evolution.

● End-to-End (E2E): System-level solutions, such as power supply, air conditioning, lightning protection, and firefighting, equipment-level solutions, such as network, IT, and security devices; plus unified Network Management System (NMS).

● Data Center (DC): Single cabinet MicroDCs; containerized DCs; modular DCs that support quick installation and smooth expansion; traditional DCs for rack space deployment.

● Resource management and disaster recovery: Unified and resilient, distributed cloud DCs.

● Intelligent Monitoring Platform.

● Video Monitoring Systems (VMS): Support cameras from different vendors and shared access to social video resources. Video resources are stored and shared across locations, departments, and types with a global catalog view. VMSs provide fast, secure, distributed cloud data storage with real-time content viewing of large-scale videos and query response times in seconds.

● Video Content Management (VCM) provides parallel and structured cloud computing. Big Data, and the Internet of Things (IoT), is the foundation of the Huawei Safe City architecture.

The core products and services for the Huawei Safe City solution include:

• FusionSphere: Distributed Cloud Platform

• OpenStack-based Cloud OS: Services feature high compatibility and capability for continuous evolution.

• Video Monitoring Systems (VMS): Support cameras from different vendors and shared access to social video resources. Video resources are stored and shared across locations, departments, and types with a global catalog view. VMSs provide fast, secure, distributed cloud data storage with real-time content viewing of large-scale videos and query response times in seconds.

• Video Content Management (VCM) provides parallel and structured cloud computing. Big Data, and the Internet of Things (IoT), is the foundation of the Huawei Safe City architecture.

The Huawei Safe City solution constructs an open ecosystem with customers and industry partners. >>

Building an Open Platform for Safe Cities

By Bai Jianhua, General Manager, Government Solutions, Enterprise Business Group, Huawei Technologies Co., Ltd.

S

tolving complex crimes in heavily populated urban centers requires advanced security technologies and an adequate police force. Public security agencies are now exploring Safe City platforms that use the latest security technologies to improve efficiency, high-tech crime detection, and crime prevention, and expand police services on demand.

Open, Decoupled, and Modularized

Most Safe City systems today are highly customized solutions involving multiple vendors. Service upgrades on such legacy systems are costly and time consuming. An additional complication is vendor lock-in. Although the old system may feature converged elements (terminals, networks, services), what it lacks is an open, decoupled, and modularized platform.

By Bai Jianhua, General Manager, Government Solutions, Enterprise Business Group, Huawei Technologies Co., Ltd.

An additional issue is the cyberspace domain, as opposed to the physical realm. Traditionally, government departments have their own Com-
analysis of the characteristics of extensive video recordings and large-capacity, high-performance cloud-based analysis of videos, including: 1) Video analysis across locations and tasks, dynamic delivery of tasks, local data analysis, and converged results using distributed cloud architecture; 2) Edge nodes such as intelligent IP Camera (IPC) connected to central VCM servers; 3) Dynamic loading of intelligent algorithms to complete analysis tasks, and 4) VMS, video analysis algorithms, and service systems from different vendors.

- Converged Communication Platform

Integrated Communication Platform (ICP) supports:

- Multi-channel incident reporting and technical protection alarms interconnected with an IoT security platform and video surveillance alarms
- Converged interconnections of various resources, such as landline phones, mobile phones, narrowband/broadband trunking, IP phones, video cameras, and other video sources
- Open Application Platform Interfaces (APIs) to simplify interconnections with service providers

The ICP provides:

- Converged voice, video, and data communication services to improve dispatch efficiency
- Multi-mode conferences, network videos, Geographic Information System (GIS), Global Positioning System (GPS), police databases, and third-party data sources
- Site visualization based on 4G/eLTE wireless broadband trunking, IP phones, video cameras, and other video sources
- Open Application Platform Interfaces (APIs) to simplify interconnections with service providers

The ICP provides:

- Converged voice, video, and data communication services to improve dispatch efficiency
- Multi-mode conferences, network videos, Geographic Information System (GIS), Global Positioning System (GPS), police databases, and third-party data sources
- Site visualization based on 4G/eLTE wireless broadband trunking, IP phones, video cameras, and other video sources
- Open Application Platform Interfaces (APIs) to simplify interconnections with service providers

- Video surveillance tools to design service flows for different alarms
- REST interfaces that enable upper-layer service development
- Lightweight, low-power, self-configuring IoT OS and development environment for embedded IoT devices
- IoT agents and gateways to simplify network access for sensors from different vendors using different protocols

The IOT Security Management Platform supports:

- Multiple communication protocols for sensor access
- Invoking communication capability of ICP platform for efficient coordination
- Fault-tolerant Big Data Platform

FusionInsight provides:

- Unified data access facilitates extension of data sources
- Unified Management Platform

The Unified Management Platform supports:

- Unified management of network, servers, security, storage, and DC equipment rooms to improve Operations and Maintenance (O&M) efficiency
- Professional knowledgebase and E2E analysis procedures based on historical fault statistics
- The Unified Management Platform supports:
  - Access management for third-party devices
  - Integrated management of cameras sites and increasing use of full-field-of-view cameras to enhance online availability of live images

Unified Security Platform

The Unified Security Platform provides:

- Unified security management at cloud, pipe, and device levels to ensure equipment and service-level security
- Security architecture, management configuration, and advanced security protections
- Multiple access authentication and session controls, blocked access from invalid cameras
- Unified Security Platform supports:
  - High security passwords to prevent videos from going public

Safeguarding the Future

Safe City constructions and maintenance require R&D competency and long-term investment. Huawei has 10 R&D centers worldwide and invests over 10 percent of its annual income in R&D. Since 2015, Huawei has focused on Safe City solutions to promote fast commercial deployment and continuous innovation of its Safe City platform. By advancing Safe City system architecture and ICT technologies, Huawei builds open, compatible Safe City solutions that support smooth evolution and continuous innovation for customers. Huawei is committed to helping customers build an ecosystem that encourages cooperation with different vendors to improve technology, efficiency, and value through service innovation. The Huawei Safe City solution is now serving 400 million people from more than 30 countries, including China, Kenya, Saudi Arabia, and Indonesia. ▲
An Evolution in Public Safety Networks

By Mao Xinjun, Chief Engineer, Wireless Marketing Department, Enterprise Business Group, Huawei Technologies Co., Ltd.

Traditional analog and digital trunking networks were not built with the demands imposed by modern public safety systems, such as Global Positioning System (GPS) inputs, new media data types, and channel congestion capable of crashing the system. Among the primary sources for these problems are cellular base stations that are limited to 4,000 subscribers per station, a 25 KHz channel bandwidth, and a 28.8 Kbit/s transmission rate. Legacy trunking systems are not equipped to support the transmission of multimedia video, Big Data, or any other Safe City service that requires a high-bandwidth channel.

To answer the call, Huawei’s Public Safety enterprise Long-Term Evolution (PS-eLTE) platform features high channel bandwidth (5/10/20 MHz), data throughput at speeds up to 100 Mbit/s, as well as:

- Real-time and non-real-time video transmission for obtaining video images of crime scenes or disaster sites taken by drones, vehicle-mounted cameras, and wearable police cameras
- Remote database access for instant retrieval of identification verification, including driver’s licenses and criminal records; obtaining medical records before a patient has arrived at the hospital; or performing telemedicine with the aid of real-time video transmission
- Image transmission for sending relevant images to on-site police officers or building blueprints to the fighters
- Biological feature identification for assisting police officers to identify suspects or survivors using fingerprint identification, facial comparison, or iris scanning

Construction Prerequisites

LTE network standards have evolved in clear and distinct steps from early 1G and 2G platforms to the 4G and 5G solutions that are available today. The following prerequisites are necessary for the construction of any large-scale PS-eLTE network today:

- LTE Standard Definitions
  In Q1 2017, the 3GPP is scheduled to release the R14 version of LTE and define other PS-LTE-based features, such as urgent video and data.
  In March 2016, 3GPP released the R13 version of the LTE specification that defined Mission-Critical Push-To-Talk (MCPTT), isolated E-UTRAN Operation for Public Safety (iEPS), and Group Communication System Enablers for LTE (GCSE_LTE) and Proximity Services (ProSe).
  In Q1 2017, the 3GPP is scheduled to release the R14 version of LTE and define other PS-LTE-based features, such as urgent video and data.

- Mobile network operators like Verizon (U.S.), EE (U.K.), KT (South Korea), and Telstra (Australia) are engaged in PS-LTE network construction projects to attract customers and expand commercial coverage.
- Service applications. Huawei, Ericsson, NOK, Samsung, ZTE, and other commercial network vendors provide market-ready solutions to the PS-LTE market; consulting firm Hexagon completed its interface adaptation to the PS-LTE network and now offers services and applications required by public safety users worldwide; and Qualcomm and HiSilicon will provide chip and module solutions following the release of new, related standards. Meanwhile, technical requirements and costs of terminal manufacturing are decreasing.

- The Industry Chain
  Reaches Maturity
  PS-LTE solutions are developing rapidly in converged platform, pipe, and terminal service applications. Huawei, Ericsson, NOK, Samsung, ZTE, and other commercial network vendors provide market-ready solutions to the PS-LTE market; consulting firm Hexagon completed its interface adaptation to the PS-LTE network and now offers services and applications required by public safety users worldwide; and Qualcomm and HiSilicon will provide chip and module solutions following the release of new, related standards. Meanwhile, technical requirements and costs of terminal manufacturing are decreasing.

- The Industry Chain
  Reaches Maturity
  PS-LTE solutions are developing rapidly in converged platform, pipe, and terminal service applications. Huawei, Ericsson, NOK, Samsung, ZTE, and other commercial network vendors provide market-ready solutions to the PS-LTE market; consulting firm Hexagon completed its interface adaptation to the PS-LTE network and now offers services and applications required by public safety users worldwide; and Qualcomm and HiSilicon will provide chip and module solutions following the release of new, related standards. Meanwhile, technical requirements and costs of terminal manufacturing are decreasing.

- Mobile network operators like Verizon (U.S.), EE (U.K.), KT (South Korea), and Telstra (Australia) are engaged in PS-LTE network construction projects to attract customers and expand commercial coverage.

- Service applications. Huawei, Ericsson, NOK, Samsung, ZTE, and other commercial network vendors provide market-ready solutions to the PS-LTE market; consulting firm Hexagon completed its interface adaptation to the PS-LTE network and now offers services and applications required by public safety users worldwide; and Qualcomm and HiSilicon will provide chip and module solutions following the release of new, related standards. Meanwhile, technical requirements and costs of terminal manufacturing are decreasing.

- The Industry Chain
  Reaches Maturity
  PS-LTE solutions are developing rapidly in converged platform, pipe, and terminal service applications. Huawei, Ericsson, NOK, Samsung, ZTE, and other commercial network vendors provide market-ready solutions to the PS-LTE market; consulting firm Hexagon completed its interface adaptation to the PS-LTE network and now offers services and applications required by public safety users worldwide; and Qualcomm and HiSilicon will provide chip and module solutions following the release of new, related standards. Meanwhile, technical requirements and costs of terminal manufacturing are decreasing.

- Mobile network operators like Verizon (U.S.), EE (U.K.), KT (South Korea), and Telstra (Australia) are engaged in PS-LTE network construction projects to attract customers and expand commercial coverage.

- Service applications. Huawei, Ericsson, NOK, Samsung, ZTE, and other commercial network vendors provide market-ready solutions to the PS-LTE market; consulting firm Hexagon completed its interface adaptation to the PS-LTE network and now offers services and applications required by public safety users worldwide; and Qualcomm and HiSilicon will provide chip and module solutions following the release of new, related standards. Meanwhile, technical requirements and costs of terminal manufacturing are decreasing.

- The Industry Chain
  Reaches Maturity
  PS-LTE solutions are developing rapidly in converged platform, pipe, and terminal service applications. Huawei, Ericsson, NOK, Samsung, ZTE, and other commercial network vendors provide market-ready solutions to the PS-LTE market; consulting firm Hexagon completed its interface adaptation to the PS-LTE network and now offers services and applications required by public safety users worldwide; and Qualcomm and HiSilicon will provide chip and module solutions following the release of new, related standards. Meanwhile, technical requirements and costs of terminal manufacturing are decreasing.
Dedicated Networks vs. Commercial Networks

The motivation to build dedicated PS-LTE networks is the need to have critical mobile video and broadband data services available to public service agencies twenty-four hours a day, seven days a week. Cities and countries with operating narrowband trunking networks can add separate broadband infrastructure that converges the two systems at the management layer. In this scenario, the broadband network may be a backup system that carries trunked voice services until the broadband network has been fully deployed throughout the region. Once certified for reliability, the trunking voice services would be transitioned to the new broadband plants. Cities and countries with little or no narrowband public service infrastructure will be best served by committing their investments to LTE dedicated networks that expand geographic coverage and provide access to the greatest number and variety of subscribers.

PS-LTE Networking Scenarios

PS-LTE scenarios are more complex than narrowband trunking environments in order to meet advanced emergency communication requirements.

- **Commercial Networks**: Using commercial carrier networks to handle public safety services; no current deployments
- **Virtual PS-LTE Networks**: PS-LTE core networks platforms user management over virtualized public safety channels shared with commercial carriers; currently deployed in the U.S. and Belgium
- **Dedicated PS-LTE Networks**: Government financed, dedicated spectrum PS-LTE networks deployed in China and some Gulf Cooperation Council (GCC) countries
- **Mixed Networks**: Combining dedicated and virtual elements with some areas served by government-operated dedicated networks and others by commercial carrier networks deployed in the U.S. and South Korea

Planning and Construction Issues for PS-LTE

The next generations of public safety radio networks are heterogeneous systems that include a LTE core network with multiple subnets and layered services. Owing to the need to leverage existing assets and maintain service continuity — and at the cost of additional complexity in the planning stages — many public safety communication networks must configure the new generation broadband components to support legacy narrowband terminals.

### Scenario Advantages Disadvantages

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commercial Network</td>
<td>Low construction and maintenance costs</td>
<td>Low reliability</td>
</tr>
<tr>
<td></td>
<td>Rapid service deployment</td>
<td>Unhardened radio security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Poor coverage in sparsely populated areas</td>
</tr>
<tr>
<td>Dedicated Virtual Network</td>
<td>Low costs because only terminals and core networks are required</td>
<td>Low reliability with unhardened radio security</td>
</tr>
<tr>
<td></td>
<td>Fast deployment by re-using carrier network</td>
<td>Poor coverage in sparsely populated areas</td>
</tr>
<tr>
<td></td>
<td>Partial QoS assurance</td>
<td>Complex Service Level Agreements (SLAs) with carriers</td>
</tr>
<tr>
<td>Dedicated PS-LTE Network</td>
<td>High information security</td>
<td>High construction cost</td>
</tr>
<tr>
<td></td>
<td>High network reliability</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security hardened wireless base stations</td>
<td></td>
</tr>
<tr>
<td>Mixed Network</td>
<td>Wide public network coverage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Additional coverage from dedicated networks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>High QoS, hardened security, and reliability in areas of dedicated coverage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Moderate QoS, security, and reliability in areas of commercial network</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Complex SLAs with carriers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Complex architecture to ensure service continuity and consistency across networks</td>
</tr>
</tbody>
</table>
Integrating Video and Intelligence for Safe Cities

By Dr. Luo Lijun, Chief Designer, Video Surveillance Product Line, Enterprise Business Group, Huawei Technologies Co., Ltd.

Community security disruptions have reached unprecedented levels. As the European refugee crisis escalates and international security worsens, Safe City experts are adopting strategies to quickly predict, detect, and defend against security threats.

End-to-End Security

Today’s Safe City video surveillance resources are not fully shared, and security capabilities remain insufficient. Separate construction of internal and external networks for public security systems prevents internal networks from sharing data with their outside counterparts. Today’s Safe City video surveillance resources are not fully shared, and security capabilities remain insufficient. Separate construction of internal and external networks for public security networks are enhanced by video use but, in order to transfer internal video efficiently to external networks, much of the police cloud data and Big Data must also be transferred. Before such transfers can take place, End-to-End Security must be implemented.

DDoS attacks targeting important application systems

Identity or permissions misuse by different departments sharing applications

Trojan horses from external websites

The critical question in Safe City construction is how best to help police departments quickly search through vast amounts of video data for valuable leads and needed evidence to close cases: The three keys to successful searches are image quality, speed, and accuracy, all of which are determined by the efficiency of intelligent analysis algorithms.

To make intelligence ubiquitous and omniscient, high-definition camera platforms must be mounted to afford the widest possible range of motion to avoid blind spots; transmissions must be immediate, secure, and reliable; and cloud analysis must be accurate and produce fast response times. The capability to create fully connected, respective Safe City networks requires the support of high-performance hardware platforms. Network-wide intelligence supports all terminals on a network with intelligent features. This allows forward-end cameras — independently or in combination with platforms — to detect targets or recognize features in people, vehicles, and objects, and analyze complex actions.

The migration towards intelligent networks and the development of built-in intelligence can be divided into three levels:

Simple intelligence, such as the analysis of complex actions

Complex video intelligence, such as motion analysis, target detection, and the extraction of key frames or target features

Deep video intelligence, such as the analysis of target features

The industry is moving towards deep intelligence, but the main obstacle is how to layer and coordinate front-end and back-end intelligence.

The core value in security intelligence lies in its ability to alleviate the pain points of industry users. Network-wide intelligence centered on solving cases and maximizing public security enables police to examine cases and make decisions efficiently due to the following features:

- Video clues allow facial and license plate recognition and tracking of people and vehicles.
- Linearly expandable distributed architecture and dynamically adjustable distributed computing provide fast, concurrent video downloads and high video compression.
- Information can be retrieved in seconds from databases with trillions of records.

Linear Scalability

As 4K and 8K cameras become commonplace, more efficient encoding and decoding algorithms are needed to lower bandwidth and storage resource consumption and decrease investment. Along with these advances comes the linear scalability of systems and associated requirements.

- Distributed resource management involves the internal computing, storage, and network
The growth of urban economies and the development of strong social systems depend greatly on the maintenance of public safety and reduction of crime. The goal of the Huawei Safe City program is to provide the highest levels of security to safeguard people’s lives and property. We recognize the need for city governments worldwide to modernize their information and communication infrastructures for the purpose of implementing state-of-the-art Safe City solutions.

**IoT-connectivity**

Public safety concerns over violence, extremism, and natural disasters compel municipal governments to invest in innovative Safe City products and technologies. And, in response to market demand, technology manufacturers have developed a systemic approach for Safe City construction that features digitalized high-definition video and intelligent analytics.

Video platforms have evolved from closed, special-purpose workstations to open and shared information systems optimized to support cross-department command and control, and proactive detection to prevent incidents from occurring in the first place.

In addition to improving public security, Safe City systems are designed to support early warnings for human-generated disasters like war, terrorism, and environmental pollution — including effective management of the aftermath.

---

**Interconnection and Data Sharing**

In most Safe City construction, platforms for intelligent analysis remain separated. The lack of an open standard for southbound and northbound interfaces across intelligent platforms prevents product chains from dividing tasks precisely. This means computing resource sharing and reduces security system efficiency.

Intelligent analysis platforms must be sufficiently open; southbound interfaces must support different manufacturers’ algorithms through unified, standard-ized ports; and northbound interfaces must provide application calls and searching on upper levels through unified services or standardized ports.

Open data sharing involves creating a structured video analysis U2S networking platform that is multi-class, multi-area, and uses a layered architecture. U2S platform networking includes:

- **Metadata descriptions standards in which different types of intelligent devices and algorithms produce standard descriptions of metadata**
- **A custom, unified interface standard that decouples algorithms from platforms to create common resource pools**
- A U2S networking standard between U2S and U2S, or U2S and third-party applications, including standard interfaces for task management, alarm notifications, and metadata management

---

**Ubiquitous and Omniscient**

The continuing growth of Safe City deployments around the world comes with new requirements for large-scale intelligent service applications. From a systems design standpoint, these requirements include upgrading E2E (camera-to-network-to-platform, also known as cloud-to-pipe-to-terminal) system security, U2S analysis, linear scalability, network interconnection, and data-sharing capabilities.

High-definition video, home security, cloud services, and other advances will become deeply integrated with other new technology concepts. By creating ubiquitous, omniscient networks, we can provide intelligent data mining and sharing for all types of commerce in Safe and Smart Cities. Most importantly, with leading new ICT, we can improve communication to ensure public safety.

---

**Cities of the future will require multi-dimensional security systems that coordinate event handling with surveillance and early warning alarms.**

---

**Building Smarter Safe Cities with the IoT**

By Li Qiang, Software Architect, Safe City Solutions Team, Huawei Technologies Co., Ltd.
Video surveillance alone cannot satisfy all the requirements for Safe City services. Cities of the future will require multi-dimensional security protection based on the Internet of Things (IoT), which can connect all devices in order to implement comprehensive sensing. Connecting security systems facilitate enhanced analytics and prediction, and faster responses when handling emergencies.

Key Technologies Involved

The IoT is the engine powering the emergence of fully connected safety and security systems. The industry is geared up to meet the requirements for user-friendly intelligent service applications through IoT-connected solutions. Connecting management systems built on a number of the following technologies:

- **Multi-Service Integration:** IoT-connected subsystems, including video surveillance, access control, perimeter, and fire alarm systems, are connected and centrally managed. Powerful access control capabilities are used to integrate these subsystems at the data, signaling control, media transmission, and terminal application layers.

- **Large Sensor Populations:** Safety and security systems rely on a large number and variety of sensors to collect information from the physical world. Depending on the desired functionality, sensors will vary in physical form, function, connection mode, and data format. Management and maintenance techniques, for large numbers of sensors require parsing, format conversion, and storage configurations for the massive amounts of information collected.

- **Rule-Based Coordination:** When an alarm or emergency is reported, an IoT-connected safety and security system performs step-by-step, coordinated handling based on preset rules that specify the actions to be taken by associated subsystems in various circumstances.

- **Visualized Command and Dispatch:** An IoT-connected safety and security system displays 2D and 3D graphical information about emergency and storage configuration for the massive amounts of information collected. Depending on the desired functionality, sensors will vary in physical form, function, connection mode, and data format. Management and maintenance techniques, for large numbers of sensors require parsing, format conversion, and storage configurations for the massive amounts of information collected.

Safety and Security Solution

As a leading ICT solutions provider with an in-depth understanding of customers’ Safe City service needs, Huawei has developed an IoT-connected safety and security solution based on its mature, industry-leading converged solution premises. The solution is built on an array of Huawei’s in-house technologies, including IoT access gateways, Big Data analytics, and cloud computing. Additionally, it leverages the industry’s advanced Physical Security Information Management (PSIM) technology and open Representational State Transfer (REST) architectures for distributed components. These combined technologies deliver a highly reliable IoT platform that features intelligent sensors, ubiquitous connectivity, and enhanced security.

The Huawei IoT-connected Safety and Security Solution is divided into four logical layers: terminal, access, platform, and application. The terminal layer is composed of intelligent hardware and various types of sensors that collect and forward data to log, control, and link information displays about on-site situations. Huawei has collaborated with industry-leading partners to provide off-the-shelf devices at the terminal layer that meet the needs of customers in different industries. At the access layer, Huawei provides proprietary IoT-access gateways and IoT-agent software components to access terminal devices in different scenarios. Upstream gateways support various wired and wireless network access modes. Downstream gateways provide common interfaces that support rich standards and specifications, including Bluetooth, Near-Field Communication (NFC), Infrared Data Association (IrDA), Wi-Fi, ZigBee, and RS232/485. Custom interfaces are available for customers with special access requirements to the terminal layer. IoT agent components can be deployed on third-party gateways running Linux or Android systems.

The platform layer consists of two parts: the IoT-platform and service platform. The IoT platform accesses and manages all terminal devices. It supports real-time data collection and analysis about the status of intelligent terminal devices, alarms, and events, including event prediction. It also supports rule-based alarm and hierarchical linkage. The service platform employs PSIM technology as its implementation functionality such as event scheduling, alarm management, and coordinated service processing between subsystems. The service platform collaborates with the GIS to support visualized alarm and equipment resource management. The entire platform layer supports cloud-based deployment and adopts the REST architecture for unified Web service interfaces between upper-layer applications and platforms.

The application layer consists of third-party applications, such as the Computer-Aided Dispatch (CAD) and Pushing Big Data Analytics (PBDA) platforms. Using the web interfaces provided by the platform layer, the application layer obtains the platform capabilities and resources needed to implement third-party services.

Broad Market Prospect

Safe City platforms come with extensive requirements and applications. The Huawei IoT-connected Safety and Security Solution can be integrated with a CAD subsystem in an existing Safe City environment to add functionality, such as an early warning component or to provide new connectivity between resources. In Africa, the Huawei solution was deployed to help Kenya build a national security surveillance, communications, and control system. With this system, Kenya improved its public security infrastructure and created favorable conditions for further economic development. The Huawei IoT-connected Safety and Security Solution can be deployed as separate modules to implement stand-alone security, surveillance, or management platforms. These platforms ensure the safety and security of important areas such as borders, government premises, military bases, and industrial parks.
Cloud Data Centers Improve Police Performance

By Li Jun, Marketing Manager, Enterprise Business Group, Huawei Technologies Co., Ltd.

Information Technology (IT) is playing an increasingly important role in maintaining public security and social order. Police departments worldwide are challenged by insufficient investment in IT infrastructure, incompatible software and hardware, and poor interoperability of their legacy systems. Obsolete technology not only wastes resources but also fails to meet the growing demands of police work worldwide. Using Software-Defined Networking (SDN), the DC solution enhances the data processing capabilities of police IT systems.

Flexible Service-Driven IT

Huawei’s Cloud Data Center (DC) operating system, based on the growing demands of police work worldwide. Using Software-Defined Networking (SDN), the DC solution enhances the data processing capabilities of police IT systems.

Data-Driven Systems

Legacy police IT systems have been designed to support structured data, such as in the 200 TB of公安 surveillance cameras deployed throughout a medium-sized city, or the minimum of 20 million surveillance cameras deployed throughout a medium-sized city, or the minimum of 20 million video data captured daily by the ten thousand video surveillance cameras deployed throughout a medium-sized city, or the minimum of 20 million video data captured daily by the ten thousand video surveillance cameras deployed throughout a medium-sized city, or the minimum of 20 million video data captured daily by the ten thousand video surveillance cameras deployed throughout a medium-sized city, or the minimum of 20 million video data captured daily by the ten thousand video surveillance cameras deployed throughout a medium-sized city, or the minimum of 20 million video data captured daily by the ten thousand video surveillance cameras deployed throughout a medium-sized city, or the minimum of 20 million video data captured daily by the ten thousand video surveillance cameras deployed throughout a medium-sized city, or the minimum of 20 million video data captured daily by the ten thousand video surveillance cameras deployed throughout a medium-sized city, or the minimum of 20 million video data captured daily by the ten thousand video surveillance cameras deployed throughout a medium-sized city, or the minimum of 20 million video data captured daily by the ten thousand video surveillance cameras deployed throughout a medium-sized city, or the minimum of 20 million video data captured daily by the ten thousand video surveillance cameras deployed throughout a medium-sized city, or the minimum of 20 million video data captured daily by the ten thousand video surveillance cameras deployed throughout a medium-sized city, or the minimum of 20 million video data captured daily by the ten thousand video surveillance cameras deployed throughout a medium-sized city, or the minimum of 20 million video data captured daily by the ten thousand video surveillance cameras deployed throughout a medium-sized city, or the minimum of 20 million video data captured daily by the ten thousand video surveillance cameras deployed throughout a medium-sized city, or the minimum of 20 million video data captured daily by the ten thousand video surveillance cameras deployed throughout a medium-sized city, or the minimum of 20 million video data captured daily by the ten thousand video surveillance cameras deployed throughout a medium-sized city, or the minimum of 20 million video data captured daily by the ten thousand video surveillance cameras deployed throughout a medium-sized city, or the minimum of 20 million video data captured daily by the ten thousand video surveillance cameras deployed throughout a medium-sized city, or the minimum of 20 million video data captured daily by the ten thousand video surveillance cameras deployed throughout a medium-sized city. When applied to police IT systems today, these architectural characteristics support multiple ways of confronting challenges:

• Uniform system planning at the top layer
• Hardware and software consolidation
• Sharing data across systems and departments
• End-to-end (E2E) application development
• Enhanced disaster recovery and backup
• More stable and reliable equipment rooms

Mass Data Processing

FusionSphere manages resource pools of servers and other physical devices. In the Huawei DC cloud solution, a customized Hadoop platform is used to host Big Data processes that include data query, data mining, analytics, and real-time streams of structured, semi-structured, and unstructured data.

Unified and Refined

Huawei ManageOne simplifies the Operations and Management (O&M) of Software-Defined Data Centers (SDDCs) by integrating SDN with Software-Defined Storage (SDS). The results are unified E2E solutions that boost overall performance and allow multiple facilities to be managed as a single data center.

Most medium-sized city-level police bureaus and their multiple sub-bureaus have their own data centers. Because these data centers operate independently from one another and, they were not built to support information sharing. With Huawei’s Police Cloud solution, the interconnection of geographically separated data centers can be managed in a unified way to support a broad range of police services. Through virtualization, physical data centers can be divided logically into multiple Virtual Data Centers (VDCs) to support multiple Virtual Private Clouds (VPCs). Each one of these VPCs can deliver a single type of police service, such as case investigations or traffic management.

The ManageOne solution enables the physical resources of each data center to be allocated on-demand to meet the service requirements for police department employees at different levels and from different departments. ManageOne reduces data center workloads and prevents conflicting demands for physical resources by different services.

Public Security

The Huawei Police Cloud solution has reduced roll-out times for new public services throughout China. Previously, departments required weeks to install and configure new equipment whereas Huawei’s automatic deployment functionality is designed to provision all resources within 24 hours.

The FusionSphere-DC cloud computing system supports on-demand resource allocation that facilitates application submission, which previously took days or weeks to come on line but now can be completed as little as 10 minutes. A

I
Video surveillance systems must overcome low efficiency, unreliability, and poor compatibility.>>

Video Cloud for Integration

By Xia Dasheng, Architect, Government Solutions, Enterprise Business Group, Huawei Technologies Co., Ltd.

To advance video surveillance storage systems, Huawei built its Video Cloud solution for file sharing across surveillance systems and regions. Cloud access nodes are deployed at police stations and other official sites. These virtual storage machines load Huawei or Huawei partner surveillance softwares to record, stream, fast-forward, and search. The access nodes support open stream storage, rapid convergence, and video data protection to ensure matter, stable, and reliable level-1 storage.

Also, centralized storage nodes are deployed at the data-link level in a shared pool for analysis and archival access. Storage resources are integrated with upper-layer service systems to perform multiple real-time video invocation and facial recognition services, among others. The central storage nodes ensure adequate single-system capacity and N+M backup to a resource pool of logical nodes. Parking centralized, multi-level network, Huawei’s Video Cloud solution supports multiple, flexible deployment modes. For example, small- and medium-sized cities can adopt centralized deployments while larger cities can establish control centers in several locations.

Wanted: Intelligent Video Analysis

Vast amounts of original video provide essential information to solve cases; however, traditional investigative methods waste labor and material resources. For example, in China, more than 500 police officers spent thousands of hours over a 24-hour period reviewing video in multiple formats to obtain 15 hours of relevant footage. While this example may seem extreme, human screening has long been the only available technology to do the work. Given the overwhelming numbers of available public and private video recordings, the security industry is motivated to acquire the most intelligent and efficient video analysis possible.

The Huawei Video Content Management (VCM) platform performs real-time behavioral analysis and structured processing on images sourced from intelligent video cameras and other front-end data acquisition devices. The analysis covers a range of issues from object abandonment to crowd density. This VCM platform functionality improves the effectiveness of the system to identify inciendies. The image investigation and control functions deployed at video-cloud access and central nodes support the following:

- Efficient case management incorporates data inputs, comparative analysis, and statistical management.
- Intelligent search provides a series of search conditions — location, time, action, and type — to filter large quantities of seemingly unrelated information, making it possible to quickly and accurately spot target patterns within massive video data stores.
- Video abstraction technology separates moving objects from their backgrounds and then condenses the video into clips to shorten browsing time and reveal the value of surveillance video during a criminal investigation.
- Virtual checkpoint technology enables standard cameras with a software asset to perform automated checkpoint control of license plates and human faces.

ePolice

Road safety systems in cities can generate a variety of data, including license plate information and surveillance video. ePolice and intelligent traffic system checkpoints are used to provide critical traffic management information and case detection services. The intelligent analysis functions of the ePolice system detects, captures, and records a wide range of traffic violations. The system records vehicle locations and times around the clock.

Head-on cameras autonomously capture an image of each incoming car’s license plate for upload to the command center, which then generates the identifying information for storage in a checkpoint information database for query and statistics. The command center system reports on vehicles involved in various situations.

Quick Clues

Although video clouds resolve many data-sharing and intelligent analysis issues, the public security system still faces the following challenges:

- Video information cannot automatically be matched with crime cases.
- Performance of control platform nodes has not kept pace with increased numbers of checkpoints.
- Traditional checkpoint systems support only local storage, so many municipal police departments are only able to conduct historical data analysis.

Because information is scattered across databases, multi-database operations are required to complete the analysis. To address this, Huawei has utilized Big Data technologies to perform comprehensive analysis of structured data generated from VCM and vehicle records, photos, and related data. This analysis allows for more clues to be found quickly.

The use of ‘video in the cloud’ grows more complex as its scale expands. The Huawei Video Cloud platform offers distinct advantages in handling complicated transitions. With a cross-region video cloud platform featuring multi-layer sharing and Big Data analytics, Huawei has pioneered and continues to be a leader in the field of cloud surveillance. [Focus]
Public security agencies are counting on new technologies to help solve security issues in cities large and small.>>

By Thomas Lynch, Director, Critical Communications, IHS

Urban areas worldwide have grown in population from 746 million in 1950 to 3.9 billion in 2014—over 5 times more people in just 64 years. Better jobs and financial opportunities continue to fuel this migration. However, the costs of prosperity and urbanization include pressures on city leaders to invest in adequate infrastructure solutions, including security.

Market Drivers and Enablers

The risks facing modern cities range from ‘high impact, low probability’ security threats and natural disasters to ‘low impact, high probability’ scenarios, such as petty crime. Protecting public spaces from extremist militant and lone-wolf attacks is a high priority that cannot be met by traditional security systems. The following market drivers are impacting public safety in Safe Cities:

- Security threats and extremism
- Economic growth and protection
- Data sharing
- Political motivation
- Crime
- Cost savings

In addition to these market drivers, Safe City projects require one or more enablers. These enablers include economic prosperity, economic risk, population growth, and stability. In 2015, governments worldwide spent more than USD 5.5 billion on public safety solutions and are projected to spend over USD 8 billion by 2019.

Connectivity and the IoT

Connectivity is at the core of Safe City projects in which government agencies, corporate enterprises, and, in some instances, the citizens that work and live in these Safe Cities collaborate. The Internet of Things (IoT) will significantly impact future Safe Cities due to near ubiquitous connectivity and inexpensive processing and sensor solutions. Newly connected devices and services will be integrated into a city’s control system using converged communication technology and advanced ICT platforms. New inputs—ranging from social media analysis to gunshot detection—will communicate directly to the command and control and Physical Security Information Management (PSIM) platforms. Through a consolidated IT and technology platform, cities can optimize budgets, integrate technologies, and make better informed, real-time decisions.

Intelligence Gathering

Before an event, city sensor systems proactively gather intelligence via the IoT. Sensor feeds are determined by the scope of the territory and the required interoperability for systems and data. These systems routinely include video surveillance cameras, audio and video analytics, and Chemical, Biological, Radiological, and Nuclear (CBRN) and weather sensors. Facial recognition and License Plate Recognition (LPR) platforms also play important roles in the process. Big Data solutions are well-suited for intelligence gathering through the analysis of numerous inputs from IoT sensors. Big Data platforms fuse multiple, simultaneous inputs into recognizable patterns. This analysis helps identify threats that would be missed if the system were to only monitor individual sensors.
The cloud is an effective infrastructure that is able to provide the necessary processing power to support video analytics and Big Data applications. The cloud also provides a solution for video storage, especially for body camera footage and other environments where the data payload is far out of range for any legacy system.

Video surveillance and analytics, command and control and PSIM, and Long-Term Evolution (LTE) trunking are pivotal for Safe City evolution.

Video Surveillance and Analytics
Networks of surveillance cameras protect parks, streets, parking facilities, and other public areas. Additionally, video surveillance facilitates emergency responses through live feeds that can be used by authorities to make real-time decisions.

Video analytics add intelligence via Video Content Analysis (VCA) algorithms, which detect, classify, and track predefined objects and behavior patterns. This automates monitoring to reduce human errors that are caused by fatigue. Video analytics are particularly effective in identifying events as they happen and extracting objects from the recorded video.

Historically, the video analytics market has been damaged by over-selling the technology's accuracy; however, this is slowly changing. The market is beginning to embrace new algorithms that more reliably track people, identify objects, and automatically detect changing weather conditions.

Command and Control
Control room systems are at the heart of every Safe City project. Safe City solutions integrate all security-related information onto consolidated ICT platforms that use the following technologies:

- Computer-aided Dispatch (CAD) is used to display and track resources per incident. CAD software typically relies on databases that contain street addresses and lists of units that are equipped to respond to alarms.
- Call-taking software allows Public Safety Answering Points (PSAPs) to manage incoming calls. When combined with CAD, PSAPs provide information access through a variety of user interfaces.
- GIS uses layers of geographical data to build comprehensive maps that support decision making and organize the analysis of incidents and events.
- Records management software enables each control room to accurately recall event details and form investigation targets.
- Video dispatch permits video conferencing through a console at the dispatch center. Real-time data from the scene can be incorporated into the primary command and control display.

Trunking
LTE is the primary communication network, or trunk, for Safe Cities and control room operators who must deal with increasingly larger amounts of data. Private LTE networks enable data streaming and enhance information received from first responders in the field. In some countries, public safety private LTE networks are rapidly advancing. The U.S. in particular is leading the way with FirstNet, a high-speed broadband data network dedicated to public safety. FirstNet's high-speed network uses a nationwide spectrum license that creates a single platform for public safety communications. FirstNet was built to public safety standards using LTE wireless technolog...
Safe City Market Drivers

The Safe City market is driven by various challenges and requirements, depending on the country and region.

- **Middle East**
  - Extremism remains a significant threat in the Middle East. In response, the region has been quick to adopt facial recognition, License Plate Recognition (LPR), and other new technologies. These solutions often incorporate video analytics to recognize vehicle type, make, model, and color.

- **Latin America**
  - Security threats are not the primary driver in Latin America; however, crime is a major issue. In many cities, informal settlements (some very large) suffer from above average crime rates.

- **North America**
  - Many Safe City projects in the U.S. use technologies specific to counter-terrorism. Larger cities using federal funding for Safe City projects are concerned not only with protecting their own citizens and assets but also with protecting visitors. Smaller U.S. and Canadian cities implementing cloud-based technology, however, can change project funding from Capital Expenditure (CAPEX) to Operational Expenditure (OPEX), which typically covers day-to-day operating costs. This allows money to be spent incrementally with no long-term commitment. In this way, cloud-based technology shifts the responsibility and risk away from the city and onto the provider.

Cloud-based technology, however, can change project funding from Capital Expenditure (CAPEX) to Operational Expenditure (OPEX), which typically covers day-to-day operating costs. This allows money to be spent incrementally with no long-term commitment. In this way, cloud-based technology shifts the responsibility and risk away from the city and onto the provider.

Safe City Market Drivers

The Safe City market is driven by various challenges and requirements, depending on the country and region.

- **Middle East**
  - Extremism remains a significant threat in the Middle East. In response, the region has been quick to adopt facial recognition, License Plate Recognition (LPR), and other new technologies. These solutions often incorporate video analytics to recognize vehicle type, make, model, and color.

- **Latin America**
  - Security threats are not the primary driver in Latin America; however, crime is a major issue. In many cities, informal settlements (some very large) suffer from above average crime rates.

- **North America**
  - Many Safe City projects in the U.S. use technologies specific to counter-terrorism. Larger cities using federal funding for Safe City projects are concerned not only with protecting their own citizens and assets but also with protecting visitors. Smaller U.S. and Canadian cities implementing cloud-based technology, however, can change project funding from Capital Expenditure (CAPEX) to Operational Expenditure (OPEX), which typically covers day-to-day operating costs. This allows money to be spent incrementally with no long-term commitment. In this way, cloud-based technology shifts the responsibility and risk away from the city and onto the provider.

Safe City Market Drivers

The Safe City market is driven by various challenges and requirements, depending on the country and region.

- **Middle East**
  - Extremism remains a significant threat in the Middle East. In response, the region has been quick to adopt facial recognition, License Plate Recognition (LPR), and other new technologies. These solutions often incorporate video analytics to recognize vehicle type, make, model, and color.

- **Latin America**
  - Security threats are not the primary driver in Latin America; however, crime is a major issue. In many cities, informal settlements (some very large) suffer from above average crime rates.

- **North America**
  - Many Safe City projects in the U.S. use technologies specific to counter-terrorism. Larger cities using federal funding for Safe City projects are concerned not only with protecting their own citizens and assets but also with protecting visitors. Smaller U.S. and Canadian cities implementing cloud-based technology, however, can change project funding from Capital Expenditure (CAPEX) to Operational Expenditure (OPEX), which typically covers day-to-day operating costs. This allows money to be spent incrementally with no long-term commitment. In this way, cloud-based technology shifts the responsibility and risk away from the city and onto the provider.
AI Turns Science Fiction into Reality

By Zhu Long, CEO, Yitu Technology

Computer Vision

Person of Interest is an American television science fiction series that uses an Artificial Intelligence (AI) system to monitor, analyze, identify, and predict violent crimes. Developed by billionaire genius Harold Finch, the AI operates cameras to track criminals and anticipate their actions. In addition, the system collaborates with other machines to rescue victims more quickly than humans ever could.

Artificial Intelligence has grown dramatically in the fields of speech recognition, computer vision, and language comprehension, even surpassing human beings in some cases. Today, facial and voice recognition technologies are commonly used across the globe.

In this case, the often fantastic science fiction of television and film may not be so far-fetched. Facebook’s ‘Tag Suggestions’ software automatically scans new images seeking matches with previously tagged photos. The ‘FaceMe’ smart-face recognition algorithm from Taiwan’s CyberLink Corporation may be used on mobile devices to enable people-to-people connections by matching faces with personal information available across social media networks such as Facebook, Twitter, or LinkedIn.

New Applications

Though not treated with the same public enthusiasm that was lavished on Google’s AlphaGo project, the combination of computer vision and AI is widely applied in public safety, finance, and information security. Some experts feel it is possible that advanced computer vision technologies will change the ways in which we view the world. In ways that are quite different from what the academics and philosophers have so far forecast. Already, the AlphaGo has demonstrated that the gap between machine learning and human IQ has narrowed significantly.

Expanding Human Capacities

Yitu Technology was founded in 2012 following my post-doctorate at MIT’s Computer Science and Artificial Intelligence Laboratory (CSAIL). I returned to China at that time to work with my middle school classmate Liu Chenxi, who was then project leader for Alibaba’s Aiyun Aquas Cloud Platforms. Our new company combined my skills in computer vision with his expertise in cloud computing and Big Data technology.

Yitu’s first implementation was a video-image-based vehicle identification system deployed in Suzhou, China. Right away, Yitu helped solve a burglary case involving the equivalent value of USD 15,000. After the break-in, a surveillance camera captured the suspect’s car driving away. Only 10 minutes following the incident report, the police detained the suspect by filtering car brands using the new vehicle identification system.

Yitu Technology is combining its computer vision technology with Huawei’s 20 years of accumulated ICT experience.

Yitu Teams with Huawei

After years of successful practice, Yitu appreciates the opportunity to collaborate with Huawei on the construction of advanced Safe City solutions. We at Yitu are combining our deep understanding of computer vision technology with Huawei’s decades of ICT experience. Huawei’s open ICT ecosystem is a big help for startups like Yitu that want to quickly work out reliable solutions for users. In the future, we will be able to offer services to users in more countries and build safer cities using Huawei’s global network.
Protecting Enchanted Kenya

By Shaka Kwach, Head of Special Projects, Safaricom Limited

While traversing the vast lands of Kenya, picturesque landscapes gradually unfold, and unique, awe-inspiring animals are seen sharing this land freely and harmoniously with generations of Kenyans.

The Kenyan government has been leveraging these unique natural resources since the 1970s by establishing 65 wildlife parks and promoting tourism.

Security Improvements

With the advantage of its central location on the continent, Kenya’s security has become a cornerstone for the growing economy. In particular, gains in the tourism sector have been achieved owing to increases in visitor numbers and foreign trade investments. Like many countries in the world, Kenya faces security challenges from extremism threats due to proximity of warring countries; exposure to criminal incidents driven by poverty; and traffic incidents common in any busy metropolis. Trivial security problems can create unprecedented ripple effects that could impact the national economy.

Influencing Decisions

The government of Kenya recognizes Safe City solutions as a national strategy for driving security management innovations in cities throughout the country using Information and Communications Technology (ICT). Safaricom’s leading mobile network operator partnered with Huawei to provide a Safe City solution using cutting-edge technology to address the following security challenges:

• Legacy Trunking Systems: Traditional analog circuits are vulnerable to interference from external signals that lead to unclear communications between command centers and field officers. In particular, the Terrestrial Trunked Radio (TETRA) system deployed in the capital of Nairobi and other cities supported voice-only services, without the benefits that modern video and broadband data services are able to bring.

• Interoperability: A solution was needed to provide data sharing and task interactions between city and federal agencies that are required to work together. The specifications for this complex project included the condition that multiple sources of information be interconnected to ensure the necessary collaboration between agencies — from incident identification and management to prosecution.

State-of-the-Art Solution

The first phase of the project covered the Nairobi and Mombasa counties, the two most populous in the country. Enterprise Long-Term Evolution (eLTE) public safety networks were deployed to enable field officers to stream High-Definition (HD) videos directly to the command centers for sharing among members of the emergency services teams as necessary.

Huawei’s solution considered the interoperability requirements for effective policing. For example, the Geographical Information System (GIS) connected to the dispatch system provides the locations of first responders in real-time for faster incidence coordination and responses that are equivalent to major cities in the developed world. The service levels in emergency contact centers have vastly improved with each instance that a Huawei IP Contact Center has been deployed. Kenyan citizens are now more confident that an effective response will result from their reporting incidents when using the new emergency help lines.

The Huawei delivery contract also requires that operating personnel be trained in all facets of the solution and Huawei technicians remain on-call to provide crucial first-level support.

Communications Create Safer Cities

The Kenyan Safe City project continues to be delivered in phases and is already showing immediate rewards for the National Police Service and the citizens of the country’s two most populated cities. We firmly believe that the addition of a modern security management system to any city in Kenya, and perhaps Africa at large, Safaricom continues to partner with Huawei to provide cutting-edge technical solutions that transform lives.

We firmly believe that the addition of a modern security management system to any city in Kenya, and perhaps Africa at large, Safaricom continues to partner with Huawei to provide cutting-edge technical solutions that transform lives.

First presented in ICT Insights Issue 17, this ‘Safe City’ follow-up takes a deeper look into the working partnership between Huawei and Safaricom. >>

Influencing Decisions

The government of Kenya recognizes Safe City solutions as a national strategy for driving security management innovations in cities throughout the country using Information and Communications Technology (ICT). Safaricom’s leading mobile network operator partnered with Huawei to provide a Safe City solution using cutting-edge technology to address the following security challenges:

- Legacy Trunking Systems: Traditional analog circuits are vulnerable to interference from external signals that lead to unclear communications between command centers and field officers. In particular, the Terrestrial Trunked Radio (TETRA) system deployed in the capital of Nairobi and other cities supported voice-only services, without the benefits that modern video and broadband data services are able to bring.

- Interoperability: A solution was needed to provide data sharing and task interactions between city and federal agencies that are required to work together. The specifications for this complex project included the condition that multiple sources of information be interconnected to ensure the necessary collaboration between agencies — from incident identification and management to prosecution.

State-of-the-Art Solution

The first phase of the project covered the Nairobi and Mombasa counties, the two most populous in the country. Enterprise Long-Term Evolution (eLTE) public safety networks were deployed to enable field officers to stream High-Definition (HD) videos directly to the command centers for sharing among members of the emergency services teams as necessary.

Huawei’s solution considered the interoperability requirements for effective policing. For example, the Geographical Information System (GIS) connected to the dispatch system provides the locations of first responders in real-time for faster incidence coordination and responses that are equivalent to major cities in the developed world. The service levels in emergency contact centers have vastly improved with each instance that a Huawei IP Contact Center has been deployed. Kenyan citizens are now more confident that an effective response will result from their reporting incidents when using the new emergency help lines.

The Huawei delivery contract also requires that operating personnel be trained in all facets of the solution and Huawei technicians remain on-call to provide crucial first-level support.

Communications Create Safer Cities

The Kenyan Safe City project continues to be delivered in phases and is already showing immediate rewards for the National Police Service and the citizens of the country’s two most populated cities. We firmly believe that the addition of a modern security management system is the start of a new chapter in Kenya, and perhaps Africa at large. Safaricom continues to partner with Huawei to provide cutting-edge technical solutions that transform lives.
By Wu Yubin, Independent Economist

The recent tragedies in Paris, France and Brussels, Belgium have spurred government agencies worldwide to analyze their public security systems to better anticipate and respond to unexpected crises.

In June 2013, I published an article in Lianhe Zaobao, explaining that the time has come for public officials to maintain security and social order by harnessing the power of Big Data analytics. Big Data platforms, such as the PRISM surveillance program used by the U.S. National Security Agency (NSA), provide the power of Big Data analytics to track extremist leaders and take preemptive action to protect their national interests.

Improving Efficiency

For national security authorities around the world, resolving the following challenges is top of mind:

- Preventing lone wolf and coordinated attacks by monitoring the communication and behaviors of suspicious individuals
- Assessing the plans of suspects by collecting and analyzing behavior patterns
- Using digital labels, each public service product will be uniquely identified, available at any time day or night, record its own history, display and report real-time status, and suggest optimal routes to achieve its target state.

Big Data technologies open up many possibilities for resolving these difficult issues. By analyzing data from multiple sources, security authorities are able to find correlations between seemingly unrelated data points. Though sometimes, and often quite quickly, the data points are only connected after the fact, the goal remains to predict and prevent the occurrence of all such large-scale calamities.

Police officers accustomed to manually laboring over deep intelligence audiences will no doubt encounter a big learning curve with Big Data technology. In a 2015 interview, Ronen Horowitz, former Head of the Information Technology Division of the Israel Security Agency (ISA), said that the ISA had widely used Big Data analytics to track enemies and take preemptive action to protect their national interests.

Fire Prevention

The Fire Department of the City of New York (FDNY) is another good example of how Big Data is saving lives and reducing property losses.

Responsible for maintaining inspections for over 330,000 buildings, including commercial properties and apartment complexes, the FDNY had long relied on an antiquated catalogue system to stay up to date. Each building in the city was assigned a card, which included occupancy, square footage, construction materials, and year built. Each of the 341 unit commanders was responsible for assigning each card a letter, A through E, indicating how often each building should be inspected.

In 2008, FDNY implemented a Risk-Based Inspection System (RBIS) that has since been retained to meet today’s challenges. Built on a data-analytics algorithm called FireCast and using 7,500 weighted risk factors, each district chief is presented with a daily report of the buildings at highest risk of experiencing a fire that day.

Updated in 2015, FireCast 3.0 sorts data that has been collected by 17 city agencies and the New York City’s 111 non-emergency phones reporting system, including building specifications, truth violations, and noise complaints. In the past, analyzing such large volumes of data would take months. The computational process for FireCast 3.0 takes no more than 20 minutes. Every night, powerful computers at FDNY headquarters perform a statistical analysis that assigns each building a fire risk score based on three years of historical data. Buildings with the highest risk scores are placed at the top of a to-do list for building inspections.

Enhancing Public Security

Government 4.0 describes a strong trend in European countries that forecasts connecting government agencies with public facilities, assets, and services through Internet of Things (IoT)-based networks for access by all citizens. The existence of Government 4.0 networks will radically change the way in which public services are designed, managed, and consumed. With digital labels, each public service product will be uniquely identifiable, available at any time day or night, record its own history, display and report real-time status, and suggest optimal routes to achieve its target state.

Security is the most important public service provided by governments. The PRISM and FireCast 3.0 systems are just two examples of how public services are delivered within a Government 4.0-style framework. Big Data has long been used by the U.S. and member states of the European Union to serve the largest public good, and we expect that China will soon be capable of rapid breadth and utility in service to the public sector.
To read or download ICT Insights ISP Extra in electronic form, visit
To subscribe to ICT Insights, contact the Editorial Board.

Email: ICT@huawei.com
Address: H2, Huawei Industrial Base, Bantian, Longgang, Shenzhen 518129, China
Tel: +86 (755) 28760808    (010)82882758

KILLING TIME? FIGHTING CRIME!
When policemen can monitor the city easily from multiple devices in innovative new ways, public safety management becomes more effective and both policemen and citizens can feel happier and more secure.

For more information, please visit e.huawei.com
The Road to Collaborative Public Safety

In today's digital economy, a variety of new security threats have emerged. We need to evolve from building urban security systems to enhancing collaborative public security. We must keep pace with rapid societal and technological changes, and improve security arrangements for inter-agency collaboration as well as deepen police-public cooperation.