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.
MAKE CITIES FLOURISH? MAKE CITIES SMART!

At Huawei we’re helping people to live better, by making cities work smarter. While all information and data interconnects, our information and communications technology (ICT) is able to untangle traffic, innovate teaching model, enhance electricity supply, and even make streets safer. Because we understand that by working together, we can make life better for everyone. Now, that’s smart.

For more information, please visit e.huawei.com
Leading New ICT, Making Cities Safer

By Lauren Fan, Vice President, Enterprise Business Group, Huawei Technologies Co., Ltd.

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 innovations.

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.
<table>
<thead>
<tr>
<th>[Comment]</th>
<th>Leading New ICT, Making Cities Safer</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Features]</td>
<td>Smarter Cities: Right Concept, Right Methodology</td>
</tr>
<tr>
<td></td>
<td>New Insights into Smart City Constructions for ICT Enterprises</td>
</tr>
<tr>
<td></td>
<td>Location is Everything</td>
</tr>
<tr>
<td></td>
<td>Safe Cities Need Interoperability</td>
</tr>
<tr>
<td></td>
<td>A New Paradigm for Security Operations</td>
</tr>
<tr>
<td>[Special Report]</td>
<td>The Road to Collaborative Public Safety</td>
</tr>
<tr>
<td></td>
<td>Building an Open Platform for Safe Cities</td>
</tr>
<tr>
<td>[Focus]</td>
<td>An Evolution in Public Safety Networks</td>
</tr>
<tr>
<td></td>
<td>Integrating Video and Intelligence for Safe Cities</td>
</tr>
<tr>
<td></td>
<td>Building Smarter Safe Cities with the IoT</td>
</tr>
<tr>
<td></td>
<td>Cloud Data Centers Improve Police Performance</td>
</tr>
<tr>
<td></td>
<td>Video Cloud for Integration</td>
</tr>
</tbody>
</table>
[Ecosystem]
44 Safe Cities: a Revolution Driven by New ICT

[Success]
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

Yue B No. 13154

Editors:
Catherine Du       Jeff Peng
Andy Xu           Lorra Liu
Corrine Lin       Amilia Zhang
Jing Chen          Scott Jamar
John North         Pauline Zhang
Simon Locke         David Castle
Karla Jo Ormsby    Gary Taylor
Carolyn Austin
Smarter Cities: Right Concept, Right Methodology

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

Smart 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 digitalization of each system and the atomization, 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.

**People’s Smart City needs**

- **Reliability**
  - I know I can rely on my government. It will do its best to provide a transparent process and cost-effective and useful products and services.
  - A government management service system based on transparent performance appraisal helps win trust and support.

- **Safety**
  - I want to live in a Safe City that makes me feel at ease.

- **Inclusiveness**
  - Government agencies must make safety their highest priority.

- **Community Integration**
  - I expect my city to be future-ready and promising.

- **Personalization**
  - Government agencies will use new technologies to inspire people to innovate.

- **Innovation**
  - A transparent, active, and easy-to-access dialog mechanism engages people in community and city affairs.

- **People-oriented**
  - I want to live in a city that gives me opportunities and capabilities.

- **Community**
  - A government management service system based on transparent performance appraisal helps win trust and support.

- **Inclusiveness**
  - Government agencies must make safety their highest priority.

- **Community**
  - I expect my city to provide products and services that match my habits and lifestyle.

- **Innovation**
  - I expect my city to welcome my suggestions and give me a sense of belonging.

- **People-oriented**
  - The governance model of public services shall be attentive to minorities and the underprivileged, and emphasize coordination and coexistence.
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 system. 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 a brownfield scheme for applying ICT innovations 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 innovations. 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.

**Smart City Implementation Schemes**
An ICT enterprise must choose its financing and entry methods with caution when implementing its Smart City solution, no matter what field it enters or development scheme it adopts. Once a wrong method is adopted, major implementation difficulties could ensue.

- **Financing Methods**
Currently, the typical financing methods include:
  - Sole investment from governments; Public-Private Partnership (PPP) and Build-Operate-Transfer (BOT) schemes, and sole investment from private companies.
  - 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 structure for the future cooperation between companies and governments.
• Entry Method
Smart Cities remain a new concept for governments — with implementation programs often impeded by uncertainty. ICT enterprises need to actively participate with local governments in the planning, construction, and maintenance phases to promote Smart City implementation. The following best practices are worth consideration.

- **IBM 'Smarter Cities'**
  IBM is promoting their Smart City brand and its technologies as follows:
  - Invested more than USD 50 million to provide free Smart City solutions for many cities
  - Set up an internal consultation department consisting of 150 full-time researchers
  - Launched an interactive website to promote Smart Cities
  - Initiated online and offline forums and permanent organizations around the world to promote Smart Cities

- **Siemens 'Intelligent Infrastructure'**
  Siemens is providing the following assistance to Smart City developers:
  - Established a dedicated Smart City department as one of four principal departments and an interconnected department with its own financing support division to facilitate market entry and financing
  - A focus on market expansion by setting up many localized research centers and sales centers in over 70 cities

**Huawei Smart City Solution**
Huawei provided an overall Smart City solution based on the cloud-pipe-device architecture to facilitate governance, benefit residents, and boost local economies. The solution includes many applications that target top-level consultation, overall planning, and various ICT infrastructures and industries. Huawei’s solution uses many innovative technologies, such as enterprise Long-Term Evolution (eLTE), Big Data, the Internet of Things (IoT), and cloud computing. Safe City constructions, transportation, energy, governance, education, and healthcare are among the key fields that the solution supports.

**Challenges for Smart City Constructions**
The Smart City industry is increasingly mature and able to provide clear opportunities for ICT enterprises. However, BCG believes that the Smart City industry will not achieve explosive growth before the following key issues are addressed by ICT enterprises:

- **Insufficient Investment Impedes Growth**
  **Cause:** Local governments are reluctant to continue the usual practice of debt financing; ICT enterprises face an increasingly large challenge.
  **Insight:** To obtain sufficient capital, ICT enterprises must improve their own financing capabilities and enhance cooperation with other financing units.

- **Limited Vertical Integration Obscures Business Value**
  **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 Fast Replication**
  **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 pain points, obtain city construction requirements, and develop unified solutions that can be applied across the board.

BCG believes that industry expectations for rapid growth in the global market for Smart City deployments will not be achieved until the higher requirements listed above are met.
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!"
"What is your location?"
"I don’t know. We left London, heading south to Brighton. There are no lights
and it’s really dark. Hurry, I’m scared."

Sadly, this type of call is only too common. As a retired police officer with over
30 years of experience, I spent most of my service patrolling and dealing with se-
rious incidents on the roads of the U.K. When members of the public call for help,
very often they do not know where they are.

I 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 technolo-
gy 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-taking 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 emer-
gency call-taker. Locations are derived from mobile phone masts and signal

Location is Everything
strength to approximate the location of the calling device. In rural areas, the level of resolution can be sections of 5 km² or more. The situation for urban areas is better but not perfect, due in part to the greater density of roads and buildings.

Key Technologies
Fortunately, 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, and last three recorded locations.

- And My Android?
  Advanced Mobile Location (AML) is being installed as a standard feature on mobile handsets using the Android operating system. In late 2016, AML will become the standard for all phones using the Google platform. When a 911/112 call is made, the call-taker can request a location from the handset. A command from the call-taker initiates the GPS receiver in the phone. If the handset is located in a building, it will also activate the Wi-Fi receiver to establish the location from the Wi-Fi IP address.

- The 4G Effect
  The entry of 4G into domestic markets is also having an effect on how 911/112 information will be received. 4G-equipped cars and trucks are available worldwide, each with multiple on-board sensors and their own unique IP address. This may lead to images being transmitted or medical data being streamed in real time from vehicles. To be useful, however, the Public Safety Answering Point (PSAP) must be equipped to manage data.

  The U.K. is moving ahead with the installation of the Emergency Services Mobile Communications Program (ESMCP), the first countrywide deployment of 4G-based communications systems for emergency services in Europe. Every other European state is now watching the U.K. before committing.

Let’s Think
Although emergency call systems are entering the digital age, they are often hindered by outmoded judicial systems and work practices. We need to think differently. Digitalization requires a deeper understanding of how the emergency response process works.

  A major question for senior managers is whether to opt for a cloud-based solution or stick with traditional networks that require the acquisition of expensive infrastructure for implementing eCall platforms across the U.K. and Europe.

  As with other modern industrial sectors moving into cloud-based operations, legacy emergency services require security and resilience. For instance, the finance sector has implemented high security and fault tolerance standards that can serve as a foundation for adaptation by the emergency services sector.

  The U.K. in particular is an interesting case, where the national government has mandated that the police and fire services work together to improve the collaboration between their respective senior management teams.

Before an Incident
Important to turning information into intelligence is the ability to geo-locate and timestamp the data relevant to the user.

  For example, an officer completing his end-of-shift paperwork needs to have access to all available data for each incident encountered while on patrol. Smart mobile handsets are a primary component for how patrol officers collect and record information in real time.

  The system must anticipate and filter the information coming to the patrolling officer from disparate sources for relevance, including data
feeds from outside normal enforcement boundaries, such as social media.

**During an Incident**

The call-taker and dispatcher are trained to survey a variety of sources to compose a response. When using a Huawei Safe City solution, many of the sources will have been provided over an enterprise Long-Term Evolution (eLTE) backbone capable of carrying visual data from 4G CCTV, CCTV checkpoints, and other network-enabled enforcement systems. Automatic Number Plate Recognition (ANPR) systems are linked with intelligent databases and social media platforms to integrate these systems seamlessly into a single command and control environment.

Raw data becomes real-time intelligence for dispatchers and first responders. Automatic Vehicle Location (AVL) further boosts this intelligence for auto accidents. On arrival, first responders are able to provide an enhanced overall view 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, decide on the response, and allocate additional resources where necessary.

Command and control system quality is proven in incidents that require complex responses from multiple agencies. Today, each agency operates with its own policies and equipment. Integrated Safe City systems like those provided by Huawei create a new environment where the seamless transfer of data and information requires establishing ad hoc 4G LTE networks.

**Analysis and Review**

Post-incident management is as important as the original response but is often overlooked. With a multiple-vehicle collision, once the injured parties have been taken for medical treatment, it is likely that additional resources will be needed to ensure that all evidence is retrieved and documented, and the site is restored to normal. These activities require the participation of support agencies operating from different sets of reference data. Many types of data must be captured and analyzed in order to have a complete and accurate debriefing to understand exactly what occurred and the quality of the response; that is, what went well, what did not, and how can processes be improved?

Big Data analytics play a large part in this process. Full and comprehensive data sets — supported by large data stores and fast processing — can amplify the overall understanding of each emergency services environment. Here again, Huawei’s Safe City solutions are superbly qualified to meet the needs of the emergency services community.

**Changing Environment**

The technical environment for emergency service responses is changing rapidly — not only are improvements occurring to locate incidents quickly and accurately, but also the methods for communication are creating the biggest changes we have seen in decades.

The significance of these advances in economic terms, such as cost to deploy, cost to operate, and value received, is notable when considering the resulting improvements in the quality of day-to-day policing against a backdrop of reduced public spending. Coupled with the public’s demand for greater accountability and transparency in how emergency services operate, the initiative for Safe City solutions around the world puts Huawei at the forefront of our never-ending effort to ensure that emergency services personnel will continue to provide the right response, in the right place, and at the right time.
Safe Cities Need Interoperability

By Per Björkdahl, Chairman, ONVIF Steering Committee

Today’s Safe Cities are integrating security systems for a more comprehensive approach.

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.

In a world where technologies change quickly, this scenario is neither practical nor attractive, as users are severely limited by vendor lock-in and the cost of adding functionality over closed interfaces. Another approach that some end users and integrators take is to deploy products from a single manufacturer to facilitate system-wide integration. The decision to select a single vendor, by definition, stifles the addition of newer, better performing products from other vendors.

Enter Standards

ONVIF® — founded 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 communications 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. Our 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 forensics in which operators analyze specific incidents to collect evidence and assess future responses. Such
activities often require coordination with local, county, state, and sometimes federal law enforcement agencies. Video clips must be exported to provide authorities with the evidence necessary for suspect identification or prosecution.

The challenge for authorities in multi-vendor environments is video material in multiple formats that require different playback devices. Here, ONVIF’s standardized approach for file formats and associated playback equipment increases efficiency. The ONVIF export file specification defines the formats for forensic metadata, such as incident times and locations. When combined, these specifications enable the integration of devices in multi-vendor, Safe City security system deployments that streamline post-event investigations.

Standards organizations outside the physical security industry have also identified the necessity of multi-vendor protocols for achieving effective Safe City deployments.

- 2014: The International Organization for Standardization (ISO) and IEC issued the JTC 1 joint Smart Cities report.
- 2014: IEC 62676-1, the first international standard for Video Surveillance Systems (VSS) was released in cooperation with ONVIF.
- 2016: IEC 62676-2 and IEC 62676-3 were issued, including the incorporation of the ONVIF specification defining video transmission protocols for Web Services communication between network video clients and video transmitter devices.
- 2016: IEC 60839-11 is scheduled for release, which will include the ONVIF specification for Electronic Access Control for Alarm and Electronic Security Systems.

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 100 cities throughout Africa, Europe, the Middle East, and Asia-Pacific. One of many examples for the utility of ONVIF 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, Haikang, Axis, 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 end-point 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.▲
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:

- Serious and organized crime
- Counter-extremism
- Protection for the vulnerable in society
- Impact on global instability (current refugee migration crisis)
- Business continuity and emergency response management
- Major public safety incidents and events
- Policing of critical infrastructure

Safer City Initiatives

Police systems require greater integration to deliver more sophisticated and effective public services. Sorely 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:

- Increased 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
- More proactive monitoring of security targets and management of emerging threats
- Improved management of planned and spontaneous events
- 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 calls for assistance and emerging intelligence
- Efficient and effective policing to deliver the most value for the investment

C3iStar Platform

The overall aim of the Safe City Command, Control, Communication, Intelligence, Surveillance, Threat Assessment and Response (C3iStar) program is twofold:

A New Paradigm for Security Operations

By Dr. Amanat Hussain, Chief Operating Officer, BGS Ltd.
To modernize infrastructure, systems, and capabilities and enable police and other security and public safety agencies to proactively manage security situations

To facilitate a professional response to security incidents through more preventive and mission-focused deployment of resources

The C3iStar platform provides an integrated suite of technologies and infrastructure, along with an innovative Concept of Operations (ConOps), quality-focused processes, and staff capabilities, for real-time information and intelligence via a multimedia trunking platform to help field commanders make evidence-based decisions in critical operations. The platform also delivers better situational awareness through advanced analytics and relational databases.

The Intelligent Video Management System (IVS) and integrated command platform ensure that informed decisions are made regarding priority and the efficient allocation of resources in response to calls for assistance.

The collection of information and intelligence within police and security agencies and the ability to share this data with external agencies ensure seamless service delivery to the public and a timely, effective response. Additional capabilities include:

- Flexible operations systems that can evolve and expand with changing needs
- Increased capacity that accommodates expected future growth

A consolidated operations model that optimizes cross-agency coordination and communication, as well as effective public safety and emergency services delivery

A New Paradigm

The 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 communications 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. This capability permeates the whole organization, creating 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 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
made available to the appropriate personnel at all levels, enabling timely and effective decisions for countering criminals, extremists, and subversives.

Enhanced operational awareness allows officers and staff to see and understand current, emerging, and predicted 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 C3iStar 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 updated with information held in police data systems about previous incidents at that address as well as current intelligence pertaining to the residents, including vulnerable individuals or any other potential threats, such as a firearms license.

Similarly, officers may use secure handheld terminals with location services and augmented reality technology to help them identify policing tasks. For example, a patrolling officer who enters a given location or area is automatically alerted or reminded that a suspect lives nearby and is on bail for a serious crime and has a curfew. This scenario would permit the officer or supervisor to consider visiting the address to ensure the curfew is being observed.

The decision support platform draws data, information, and intelligence from collection systems and integrates the data to create key operational and business-knowledge products driven by strategic and tactical priorities. This capability, when linked to an appropriate task management system, creates a quantum leap forward in productivity and effectiveness by empowering officers and staff at all levels to make more informed decisions about services, interventions, and resources. All this occurs within a framework of discretion that encourages proportionate, preventive interventions.

**Multimedia Mobile Platform**

An integrated, resilient, and secure mobile multimedia information infrastructure improves police resource efficiency and officer safety outcomes through better decision support as well as enhanced intelligence and information for patrol officers, supervisors, and management. Police mobility requirements, however, are not just about rolling out mobile infrastructure or multimedia mobile devices. These technologies need to be aligned with new operating models and processes that transform the organization, along with clearly defined benefits and roles to improve efficiency and reduce bureaucracy.

- **Transforming the Organization**

A major cause of project failure in new deployments is underestimating the activities needed to transform the organization. Getting the ‘human dimension’ right ensures that policing organizations are primed to benefit from the technology changes and investment. As more police forces and security agencies around the world move toward technology- and knowledge-enabled operations, they must also address important issues regarding human factors as part of the overall project.

- **Staff Development**

In the new Safe City operations model, staff must be trained so they can perform with skillfulness, confidence, and empowerment. This means investing in staff development to help them adjust to new technologies and acquire the knowledge, skills, and capabilities to succeed in the new environment. They
must have 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.
  
  Far 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 tasking, briefing, and debriefing against threats, risks, and demands, 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 and when ‘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 out-of-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 reinforces 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.
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.

The Road to Collaborative Public Safety

By Khoo Boon Hui, Past President of INTERPOL and Retired Commissioner of Singapore Police and Koh Hong Eng, Global Chief Public Safety Expert, Huawei Technologies Co., Ltd.
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 faraway 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 vicious 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 infrastructure 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 cybercrime 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 crime. 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 “Selfie” 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 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.

Safe City
Be it against conventional threats or that arising from digital technologies, Safe City implementation remains critical globally. IHS estimated the Safe City market was worth USD 5.6 billion in 2015, and will reach USD 8.5 billion by 2019. The three key aims of Safe City are:

- 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.
- Enable key entities of a city to identify and act in real-time to security threats of any scale.

With more than 100 Safe City implementations in more than 30 countries serving more than 400 million people, Huawei’s Safe City solutions were well proven globally. Communication with real-time video in this day and age is imperative to public safety. Huawei provides such trunking capability, from backend networking to devices supporting LTE, both public (LiTRA) and private (eLTE). The devices, ranging from handsets to in-vehicle terminals, supports voice, data, and video. There is even the eLTE Rapid System, which integrates various components into a compact chassis ideal for rapid deployment in the field where limited coverage area is sufficient, especially at a disaster site after the main infrastructure has been crippled.

At the heart of Huawei’s Safe City solutions is the Integrated Communications Platform. A major challenge to inter-agency collaboration is the use of different technologies, networks, and devices. This platform supports interoperability of eLTE, and legacy TETRA and P25 devices. It can even connect to conventional telephone network and cellular network. In line with a visualized command center, this platform accepts video from multiple sources. It is also ready for the Digital Economy accepting data from the Internet of Things (IoT) and Social networking. Such voice, video, and data can then be routed to any groups of users/devices through Software-Defined Networking (SDN). This feature is critical because public safety agencies and officers form ad hoc groups based on Standard Operating Procedures (SOPs) to tackle different scenarios. The Integrated Communication Platform can also be integrated with the Telepresence & Video Conferencing technology, supporting video conference between commander, specialists, and even frontline officers.

Another crucial component of Huawei’s Safe City solutions is the Intelligent Video Surveillance, comprising Video Content Management, and Video Storage Cloud. This component can ingest video from many sources including those from Social networking. Scene
search allows one to search, for example, a white van. Video synopsis helps to ‘summarize’ many hours of video into crucial clips for human investigation. In a major crime, 3,500 hours of video were collected and video synopsis ‘summarized’ these to just 50 hours, allowing for a quick solving of the case. The Video Content Management also comes with more than 20 intelligent analytics including entity recognition, behavior, 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.

Existing Safe City implementations can be enhanced with various technologies such as Sensor-based Early Warning, Social Monitoring, Public Warning, and Smart Deployment. Sensors, or IoT, including buoys to detect Tsunami, CBRN (chemical, biological, radiological, and nuclear), and radar/electro-optics for border surveillance. Most Social networking sites, such as Facebook, Twitter, and Sina Weibo, allow third parties to connect directly for viewing non-private social postings. Alternatively, Social networks aggregators, such as Rola Security Solutions, SAP Social, Sysomos, and Xalted, aggregate data from across Social networking sites. As mentioned earlier, Huawei’s Integrated Communication Platform can ingest data from the IoT and Social.

Examples of Public Warning include the island-wide public warning siren in Singapore, and the Japan’s earthquake warning through their cellular networks. Traditionally, fire engines and ambulances are dispatched from stations. Some emergency services are now experimenting with Big Data to predict where and when their services are needed, and deploy their resources accordingly. Such Smart Deployment ensures that first responders arrive at the scene of incident in the shortest time. With the same objective for fast response, the Argentina Federal Police adopts ‘blue force tracking’ in Buenos Aires: police officers on foot patrol and police vehicles are tracked through GPS to ensure they uniformly patrol the city as planned. Such Smart Deployment allows a good police presence to deter crimes, improve police-community relationship, and respond to incidents in the shortest possible time.

Public Safety
Conventional threats to 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 response. These alone may not be sufficient to secure a sense of public safety. Also, as explained earlier, the Digital Economy is giving rise to cyber-facilitated extremism and organized crime that may not be adequately countered by a Safe City implementation.

Public Safety goes beyond current Safe City. It is about Preventing.
and Solving crimes, Reducing loss of life and property. Public Safety is also about minimizing disruption to life. Public Safety is beyond detection and response; it includes prevention and bringing life to normalcy. It encompasses digital security, health security, infrastructure safety, and personal safety. Indeed, on personal safety, when the then British Home Secretary Sir Robert Peel established the London Metropolitan Police in 1829, he said “the test of police efficiency is the absence of crime and disorder, and not the visible evidence of police action in dealing with them.”

Sir Robert Peel also said, “the police are the public and that the public are the police.” Unfortunately, this principle has not been diligently adopted by many police departments around the world for the last 180 years. In light of the Digital Economy, this principle is now even more crucial, or else law enforcement agencies risk being disrupted as explained earlier. We need to evolve from Safe Cities to Collaborative Public Safety.
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 with 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 the 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 out enforcements. For example, the U.S. Department of Transportation has to manage more than 300,000 companies that ship more than one million daily shipments of hazardous materials (HAZMAT). The Department uses a unified 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 and screening, passenger and cargo risk management, such as U.S. 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 the 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
During this phase, investigation and evidence collection are crucial for the following purposes:

- To locate victims and identify remains if there are fatalities
- To identify the responsible party and ensure justice is served
- To learn from the threat, and to prevent its repeat occurrence

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.

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, and 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 imprisonment, aims to prevent the occurrence 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 a heart attack, the SCDF control room will dispatch an ambulance, and at the same time send a message to those myResponder volunteers in the vicinity. The App will also inform the volunteers 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 in real time through eLTE wireless network. In the event of an incident or crime, the police control room can access such video in 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 enabling 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; and 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 based
on open standards and even open source — the best option now being OpenStack. Huawei is a major adopter, supporter, and contributor to OpenStack. In fact, by late 2015, Huawei was in the 6th position in code contribution.

Big Data and Analytics are crucial to enable many of the functions needed under Collaborative Public Safety. Examples include Threats Identification, Predictive Policing, Border Protection, Simulation and Forecast, Sensor-based Early Warning, Social Monitoring, Smart Deployment, and Criminal Intelligence.

**Whole-of-Government Command Center**

The Collaborative Public Safety concept is applicable to all manner and scale of threats. However, Command and Control is usually exercised by agencies at the tactical level. This is why police, fire, ambulance, military, and border control usually have their own Command and 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 country, each state, province, or even major city may have such a center. During times of normalcy, such centers 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 and Control centers.

Another issue is the cyberspace domain, as opposed to the physical realm. Traditionally, government departments have their own Computer Emergency Response Team (CERT) and/or Security Information and Event Management (SIEM) centers. But with increasing complexity and scale of cyber-facilitated extremism/crime described here, countries have started to invest in National Cyber Security Operations Center (NCSOC).

NCSOC usually receives data from all these CERT/SEIM centers. The objective is for a country to detect a major attack/threat against any industry by analyzing all these streams of data via Big Data-based Network Behavior Anomaly Detection (NBAD). Examples include Israel’s Cyber Security Bureau and the U.S.’s Cyber Threat Intelligence Integration Center. It is possible for NCSOC to be independent or part of the Whole-of-Government Command Center.

**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, involving inter-agency collaboration and public-private partnership. A Safe City implementation remains critical and it is usually implemented before the other capabilities of Collaborative Public Safety.

While a Safe City has a backbone of video surveillance, LTE, and command and control solutions, Collaborate 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 Collaborate Public Safety is the Whole-of-Government Command Center, which may include a NCSOC to oversee the security of the cyberspace.
Building an Open Platform for Safe Cities

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

Solving 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 systems may feature converged elements (terminals, networks, and services), what they lack is an open, decoupled, and modularized platform.

It was not possible to build legacy architectures to support the types of rapid innovation that are available today. The technological maturity of our modern solutions allows public security agencies to require open and decoupled support for southbound interfaces to access devices from multiple vendors and northbound interfaces for service optimization. With such a platform, public security personnel can quickly replace existing terminals or add new ones without having to perform large-scale adaptations or service system optimizations.

Converged, Intelligent, and Open Safe Cities
Advanced Information and Communications Technology (ICT), including 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
- **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 in equipment rooms
- **Resource management and disaster recovery**: Unified and resilient, distributed cloud DCs
- **Intelligent Monitoring Platform**
- **Video Monitoring Systems (VMSs)** 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 concurrent viewing of large-scale videos and query response times in seconds.
- **Video Content Management (VCM)** provides parallel and structured
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 Cameras (IPCs) connected to central VCM servers; 3) Dynamic loading of intelligent algorithms to complete analysis tasks; and 4) VMSs, video analysis algorithms, and service systems from different vendors.

- **Converged Command 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-node 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 technology and resource visualization by interworking with GIS
    - Voice and video communications services using Representational State Transfer (REST) service interfaces
  - **IoT Security Management Platform** provides:
    - Access management, authority control, security management, data conversion, and storage for sensor inputs

- **FusionInsight Big Data Platform**
  - FusionInsight provides:
    - Full-stack capabilities using multiple Massively Parallel Processing Database (MPP DB) platforms such as Hadoop, Spark, and Storm
    - Standard Structured Query Language (SQL) queries for smooth interconnection with traditional applications
  - FusionInsight supports:
    - Algorithms such as community discovery, route tracking, relationship analysis, and ‘similar to’ case analysis
    - Unified data access using interface adaptation layer to shield differences between various data sources to people and machines
Unified data access facilitates extension of data sources

**Unified Management Platform**

The Unified Management Platform provides:

- 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 scenarios

The Unified Management Platform supports:

- Access management for third-party devices
- Integrated management of camera 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 consultation, and advanced security protections
- Multiple access authentication and session controls, blocked access from invalid cameras

The 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 16 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 developments, 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 innovations. 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

Next-generation broadband LTE networks must be green-lighted to keep pace with the demand for having critical Safe City trunking systems available for day-to-day policing. >>
• Image transmission for sending relevant images to on-site police officers or building blueprints to firefighters
• 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 4.5G solutions that are available today. The following prerequisites are necessary for the construction of any large-scale PS-LTE network today:

● LTE Standard Definition
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 (IOPS), and Group Communication System Enablers for LTE (GCSE_LTE) and Proximity Services (ProSe).

In 2014, China Communications Standards Association (CCSA) formulated TD-LTE-based Broadband Trunking Communications (B-TrunC) standards that were later adopted by the International Telecommunication Union (ITU). In 2012, the U.S. Federal Communications Commission (FCC) allocated the 700 MHz Public Safety Spectrum using two 10 MHz B14 frequency segments. The U.K. and Spain have also released their own 700 MHz scenarios. A number of countries in South Asia are actively planning PS-LTE deployments. South Korea is preparing a 700 MHz, B28 scenario for release. China has released a 4.5G LTE-Advanced Pro, 1.4 GB 20 MHz scenario for public service networks.

● The Industry Chain Reaches Maturity
PS-LTE solutions are developing rapidly in converged platform, pipe, and terminal service applications. Huawei, Ericsson, NSN, Samsung, ZTE, and other commercial network vendors provide mature pipe-layer 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.

● Carriers Lower Difficulty of PS-LTE Network Construction
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. Infrastructure resources, availability of physical sites, O&M expertise, and professional technical staff are tools that carriers use to meet the challenges of PS-LTE network construction:

• Built cell by cell to balance service capacity and coverage, LTE networks are more complex and have more Network Elements (NEs) than traditional narrowband trunking systems.

• Compared to older, narrowband systems, LTE networks have a smaller effective range and a higher radiated spectrum that is often in the 400 MHz range. Therefore, PS-LTE networks require about four times more base stations than a narrowband system for the same number of users.
Planning, construction, and Operations and Maintenance (O&M) of PS-LTE networks present a higher set of requirements for management organizations and personnel.

Here Comes PS-LTE Construction

By the end of 2015, more than 1,000 PS-LTE base stations were in service for over 100,000 users.

- In 2012, the U.S. Congress authorized USD 7 billion to build the First Responder Network Authority (FirstNet), an interoperating national public safety broadband network.
- The U.K. began building a broadband national public safety LTE network in 2015, with a first-phase investment of GBP 1.2 billion (USD 1.65 billion); the British government plans to complete the construction by 2025.
- Kenya began building its national PS-LTE network in 2014 and completed first-phase construction of over 100 base stations and 7,000 terminals covering Nairobi and Mombasa.
- In 2013, China began building a national PS-LTE network covering more than 10 cities, including Beijing, Shanghai, Nanjing, Shenzhen, and Guangzhou; 256 base stations and over 10,000 terminals are in service in Nanjing.

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 communications networks must configure the newer generation of broadband components to support legacy narrowband terminals.

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. Areas beyond the coverage of dedicated PS-LTE networks are often supplemented with commercial networks.

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 narrowband 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 communications requirements.

- **Commercial Network:** Using commercial carrier networks to handle public safety services; no current deployments
- **Virtual PS-LTE Network:** PS-LTE core networks perform user management over virtualized public safety channels shared with commercial carriers; currently deployed in the U.K. and Belgium
- **Dedicated PS-LTE Network:** Government financed, dedicated spectrum PS-LTE networks; deployed in China and some Gulf Coop-
<table>
<thead>
<tr>
<th>Scenario</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| Commercial Network| • Low construction and maintenance costs  
• Rapid service deployment                                                  | • Low reliability                                           
• Unhardened radio security                                           
• Low Quality of Service (QoS)                                         
• Poor coverage in sparsely populated areas                             |
| Dedicated Virtual Network| • Low costs because only terminals and core networks are required  
• Fast deployment by re-using carrier network  
• Partial QoS assurance  
• High information security                                            | • Low reliability with unhardened radio security  
• Poor coverage in sparsely populated areas  
• Complex Service Level Agreements (SLAs) with carriers |
| Dedicated PS-LTE Network| • Complete QoS assurance  
• High information security  
• High network reliability; security hardened wireless base stations  | • High construction cost                                                     |
| Mixed Network     | • Wide public network coverage  
• Additional coverage from dedicated networks  
• High QoS, hardened security, and reliability in areas of dedicated coverage  
• Moderate QoS, security, and reliability in areas of commercial network coverage | • Complex SLAs with carriers  
• Complex architecture to ensure service continuity and consistency across networks |

- **Mixed Network:** 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. When planning and building PS-LTE networks, governments are advised to consider the following uses and requirements:

- Converged commercial and dedicated networks that integrate broadband and narrowband trunking
- Combined fixed and mobile with ground and airborne networks to ensure service continuity and improve command and dispatch efficiency
- Broadband mobile intelligent terminals to ensure service boundaries and device security
- QoS guarantees to fulfill key roles and services
- Construction policies for dedicated LTE networks to account for limited budgets and guide the expansion of coverage from large, developed cities to smaller, less developed areas with lower risk profiles

Modern public safety systems are designed to meet the demand to integrate new and old technologies for the purposes of service continuity and minimum investment.
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.

Cloud and Big Data services used for police investigations in internal 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, external public security networks must implement End-to-End (E2E) network, system, data, and application security to avoid the following risks:

- Trojan horses from external websites
- Stealing or leaking sensitive data from application systems
- Identity or permissions misuse by different departments sharing applications
- DDoS attacks targeting important application systems

Conventional video surveillance systems are clearly not enough. The image data that video surveillance systems collect and the valuable metadata derived from this data supply evidence for solving cases and serve as an information resource for all municipal services. To ensure the

Integrating Video and Intelligence for Safe Cities

By Dr. Luo Lijun, Chief Designer, Video Surveillance Product Line, Enterprise Business Group, Huawei Technologies Co., Ltd.
security of recorded data, video surveillance platforms must run on mature, stable frameworks that provide service-guarantee policies.

**Quality, Speed, and Accuracy**
In current Big Data applications for Safe Cities, video surveillance systems typically fail to meet service requirements, and computing power for Unstructured-to-Structured (U2S) analysis is generally weak. Specifically, the complexity of monitored areas in Safe Cities causes traditional intelligent analysis algorithms to send false alarms without reporting relevant information. Although groundbreaking technologies such as deep learning have already been applied to such systems, many features remain immature. To extract key information from data, police departments are forced to examine video data manually, which increases operations costs and decreases efficiency.

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, perceptive Safe City networks requires the support of high-performance hardware platforms.

Network-wide intelligence equips all terminals on a network with intelligent features. This allows front-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 maintaining 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 encompassing the internal computing, storage, and network...
resources of management platforms
  • A distributed scheduling framework for platform analysis and storage tasks to increase usage rates of related resources
  • Structured data preprocessing to unify processing of metadata output by different algorithms
  • An image information database to manage the structured, semi-structured (image features), and relevant unstructured data (images or video clips) output by algorithms
  • A distributed image search engine to offer unified, distributed search features for standardized metadata with multiple search types, including standard, fuzzy, and feature-based queries
  • U2S analysis interface to provide third-party applications with unified task and configuration management for intelligent analysis, notification management for alarms, search management, and access control for image information

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 restrains computing resource sharing and reduces security system efficiency.

Intelligent analysis platforms must be sufficiently open; southbound interfaces must support different manufacturers’ algorithms through unified, standardized ports; and northbound interfaces must provide application calls and searching on upper levels through unified SDK 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 description 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 control, 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-pipeto-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 communications 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.

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 communications 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 for emergency response, 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, extremism, and environmental pollution — including effective management of the aftermath.
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. Connected 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 information 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 configuration 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 situations. Working with a Geographic Information System (GIS), an IoT-connected system allows enhanced visibility into an incident’s location and scope of impact that presents a visualized command-and-dispatch interface to emergency operations personnel.

**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 emergency command solution. The solution is built on an array of Huawei’s in-house technologies, including IoT access gateways, Big Data analytics,
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 feed information displays about on-site situations. Huawei has collaborated with industry-leading partners to provide front-end 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. Uplink gateways support various wired and wireless network access modes. Downlink 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 trend prediction. It also supports rule-based alarm and hierarchical linkage. The service platform employs PSIM technology to implement 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-Assisted Dispatch (CAD) and Policing 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 safety, security surveillance, or management platforms. These platforms ensure the safety and security of important areas, such as national borders, government premises, military bases, and industrial parks.
Information Technology (IT) is playing an increasingly important role in maintaining public security and social order. Police departments the world over are challenged by insufficient investment in IT infrastructure, incompatible software and hardware, and poor interoperability of their legacy systems. Outdated technology not only wastes resources but — because obsolete systems are typically siloed by department — also creates extra work for busy officers who need to collaborate with officers in other locations or in different roles to complete their assignments.

Data-driven Systems

Legacy police IT systems have been designed to support structured data, such as the 200 TB of data captured daily by the ten thousand video surveillance cameras deployed throughout a medium-sized city, or the minimum of 20 million checkpoint records for cities with 5 million vehicles.

What is new are the forms of unstructured and semi-structured data from external sources, such as email, text, and social media messages. Today, data inputs from Facebook and Twitter are important references for correlating all available information surrounding an event or incident. Cloud computing systems designed to handle structured and unstructured data concurrently have become a necessary investment for police departments that intend to keep up with current best practices.

The U.S. National Institute of Standards and Technology (NIST) lists five essential characteristics of cloud computing: (1) on-demand self-service, (2) broad network access, (3) resource pooling, (4) rapid elasticity, and (5) measured service.

When applied to police IT systems today, these architectural characteristics support multiple ways of confronting challenges:

- Unified 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

**Flexible Service-Driven IT**

FusionSphere, Huawei’s Distributed Cloud Data Center (DC²) operating system, meets the growing demands of police work worldwide. Using Software-Defined Networking (SDN), the DC² platform and FusionSphere implement a virtual data center that supports automated management of physically scattered resources.

Based on OpenStack, FusionSphere enables the unified management of virtualized resource pools, physical servers, storage equipment, and networks that can be deployed based on demand.

With FusionSphere, services and functions formerly provided by independent servers run on Virtual Machines (VMs). These include Computer-Aided Dispatch (CAD) and a Geographic Information System (GIS) for the command center, the Video Management System (VMS) for the monitoring center, Business Intelligence (BI) for police investigations, and office software for detectives and patrolmen.

VMs eliminate the expense of dedicated hardware in favor of generic x86 servers packaged in high-density arrays that deliver the identical services at a fraction of the cost. Load-balancing functionality assures the efficient utilization of CPU and memory resources, and fast failover when faults occur.

**Mass Data Processing**

FusionSphere manages resource pools of servers and other physical devices. In the Huawei DC² 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 Maintenance (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 each 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 resources 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) able 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 service the 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 rollout 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-DC² cloud computing system supports on-demand resource allocation that facilitates application submissions, which previously took days or weeks to come on line but now are completed in as little as 10 minutes.▲
Video surveillance systems must overcome low efficiency, unreliability, and poor compatibility.

**Video Cloud for Integration**


The rate of deployment for Safe City solutions is growing in part due to advances in video surveillance storage systems.

Traditional Digital Video Recorder (DVR) and Network Video Recorder (NVR) distributed storage modes hinder resource sharing. To help, Huawei built its Video Cloud solution for file sharing across surveillance system departments and regions.

Cloud access nodes are deployed at police stations and other official sites.

These virtual storage machines load Huawei or Huawei partner surveillance software to record, stream, fast-forward, and search. The access nodes support open stream storage, rapid convergence, and video data protection to ensure mature, 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.

Featuring centralized, multi-level networks, 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 seconds 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 incidents live. The image investigation and control functions deployed at video cloud access and central nodes support the following:

- **Efficient case management** incorporates data asset 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 assist 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 assets. The intelligent analysis function 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** automatically capture an image of each oncoming 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 serious infractions.

**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.▲
Safe Cities: a Revolution Driven by New ICT

By Thomas Lynch, Director, Critical Communications, IHS

Public security agencies are counting on new technologies to help solve security issues in cities large and small. >>

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 feed this migration. However, the costs of prosperity and urbanization include pressure 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
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 communications 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 needs 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.
● Enabling Real-Time Identification and Reaction to Security Threats
City authorities must quickly identify hostile events to prevent escalation. A consolidated ICT platform provides a common operational picture to all relevant agencies — raising situational awareness and boosting effectiveness. Using converged command systems, operators have easy access to command and control systems in a single user interface. Computer-aided video dispatch, Geographic Information System (GIS), and information and data sharing vastly improve reaction times and the quality of each response.

● Post-Event Examination and Analysis
Following any given event, city authorities will quickly analyze all relevant sensor data to accelerate the investigation. Video analytics often provide a source for object metadata that is used to quickly identify search targets, such as a ‘red car’ or ‘person with a blue backpack.’ Big Data is a powerful post-event tool for correlating sensor inputs and identifying patterns of behavior.
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 overselling 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 deploy 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 communications 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 daily public safety communications. FirstNet was built to public safety standards using LTE wireless tech-
technology for greater coverage, capacity, connectivity, cyber security, and resilience compared to current multiple system solutions.

**Predictive Crime Centers**

The uptake of digital recording, evidence management, and statistical reporting from control rooms has spurred the deployment of ‘predictive crime centers.’

The convergence of Big Data in the control room is essential for transforming how dispatchers and operators manage emergencies and for gaining more statistical output from the control room. CAD platforms must be designed to facilitate this flow of information from both the caller and the first responder. Consequently, the number of CAD tenders, including a wide range of analytical capabilities and smart applications, is increasing. This is evidenced by suppliers looking for solutions that stream inputs from body cameras directly to the control room.

As users demand more-focused data, situational awareness and a user-defined operating picture are increasingly important. One challenge for the GIS/Analytics market is to hire more dispatchers to help with the overflow of information. Another challenge is the training gap. Because capabilities have expanded dramatically, successful suppliers now include training with their platforms.

**Safe Cities in the Cloud**

Software-as-a-Service (SaaS) solutions provide an alternative to fixed systems commonly installed in Safe City projects. In cloud architectures, software, applications, hardware, and storage are provided as services. Rather than committing upfront to a fixed cost, services are billed based on their rates of use; therefore, usage on a cloud network is scalable and elastic. Data can be accessed from anywhere and shared seamlessly on a much larger scale at any time across multiple devices.

One factor hindering adoption of Safe City projects is financing.
Safe Cities represent the future of urban security and safety — a future built on data, connectivity, and interoperability.

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.
  Another driver of Safe City projects in this region is economic growth. Safer cities can attract foreign investment and help diversify oil-dependent economies.

- **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.
  Natural disasters like earthquakes and landslides kill thousands of people each year in Rio de Janeiro, Brazil, and La Paz, Bolivia, due to a lack of early warning systems.

- **North America**
  Many Safe City projects in the U.S. use technologies specific to counter-extremism. 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 public safety and law enforcement projects typically forgo high-end technologies. Their primary goals are to decrease organized crime and gang activity and improve response times for emergency and non-emergency services.

- **Europe**
  The primary driver for Safe City projects in Europe is data sharing between agencies. European cities want to centralize data through a command center, which would then be used as an operations center for various stakeholder agencies. These projects generally do not use the most-advanced technology available but instead focus on integration and connectivity. The need for sharing data is driven by budget and staff cuts, counter-extremism operations, and policing and crowd management improvements.

- **Asia-Pacific**
  Developed countries, such as Australia, Japan, and New Zealand, are home to mature cities facing vastly different challenges than those in developing countries, such as China, India, and Pakistan.
  In developed markets, Safe City projects that follow similar drivers focus on sharing data to improve emergency response and counter-extremism operations.

Urban Security and Safety
Safe Cities represent the future of urban security and safety — a future built on data, connectivity, and interoperability. Cities around the world will continue to adopt smarter solutions to meet the challenges of burgeoning populations and emergency response preparedness.
Artificial intelligence has grown dramatically in the fields of speech recognition, computer vision, and language comprehension, even surpassing human beings in speech and facial recognition. 

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.

In this case, the often fantastic science fiction of television and film may not be so far-fetched. Facebook’s ‘Tag Suggestion’ 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.

Up to World Standards

The field of ‘computer vision’ began at the Massachusetts Institute of Technology (MIT) in 1966 when Marvin Minsky asked undergraduate student Gerald Jay Sussman to “spend the summer linking a camera to a computer and getting the computer to describe what it saw.” This innocent beginning led to the 1999 discovery of the Scale-Invariant Feature Transform (SIFT), which provided precise comparisons between the same object in different images.

Since then, MIT has been joined by the University of California Berkeley and England’s Oxford University as the world’s top research institutions specializing in the field of computer vision. Talented people from these universities have either been lured away by giant companies like Google or have started their own businesses.

China began computer vision research in the 1990s. Performance improvements in Big Data computing and the seamless deployment of cameras have
created the software and hardware infrastructure necessary to support China’s further development in this area. With the addition of AI, every move a person makes can be seen and future actions anticipated. With numerous Chinese startup companies in the area of computer vision, China has joined the leaders within this market segment across the globe.

**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 lives 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 is shrinking.

**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 Lin Chenxi, who was then project leader for Alibaba’s Aliyun Aspara Cloud Platform. 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 machine 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.

Face recognition will have a wider impact than vehicle identification. In a second case, the public security department in Suzhou identified 17 suspects out of 25 candidates using Yitu’s face recognition system, which produced early warnings that were generated by comparing a 100-million-image national database of criminals with images of Suzhou’s 13 million residents.

Vehicle and facial recognition technologies are also widely applied in the finance sector. For example, China Merchants Bank employs facial recognition technology in the Virtual Teller Machines (VTMs) of its 1,500 branches to open and activate accounts and perform other procedures that require identity verification. During testing, the technology proved accurate up to 98 percent of the time, while the rate of misrecognition was only 0.001 percent. The human eye can do no better than an error rate of 1 percent. In other words, machines have a far greater capacity for recognition accuracy than human beings.

**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 a combination of increases in visitor numbers and foreign trade investments. Like many countries in the world, Kenya faces security challenges from extremism threats due to the close proximity of warring countries; exposure to criminal incidents driven by poverty; and traffic incidents common in any busy metropolis. Trivial security problems can create unpredictable 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, Kenya’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 infor-
In order for information to be interconnected, it is necessary 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 Geographic 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.
Big Data for Public Security

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 coordinated criminal acts.

In June 2013, I published an article in Lianhe Zaobao, the most widely read Chinese-language newspaper in Singapore, 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 capability to share information with multiple departments quickly and precisely in response to such crises.

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 communications and behaviors of suspicious individuals
- Accessing the plans of suspects by collecting and analyzing behavior patterns
- Sharing relevant and timely intelligence across departments
- Intercepting and disrupting anonymized and encrypted communications used to cloak organizational structures and operating modes

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 archives 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 extremist leaders 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
In 2008, FDNY implemented a Risk-Based Inspection System (RBIS) that has since been refined 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 311 non-emergency phone reporting system, including building specifications, trash 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 90 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 rising 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. Government 4.0 is an echo of Industry 4.0, which is a collective term that embraces the integration of automation, data exchange, and manufacturing technologies.

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 identified, available at any time day or night, record its own history, display and report real-time status, and suggest optional routes to achieve its target state. Data capture devices, such as cameras and sensors, will be embedded ubiquitously into public facilities and secure infrastructures. IoT technologies will link public service products with real-time management systems that are able to track from the moment an order for public services is generated and captured to final delivery.

Security is the most important public service product 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 equal breadth and utility in service to the public sector.
To read or download ICT Insights ISP Extra in electronic form, visit http://e.huawei.com/en/publications/global/ict_insights

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) 28780808  (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

LEADING 

ICT IN PUBLIC SAFETY
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.

Copyright © Huawei Technologies Co., Ltd. 2017.
All rights reserved.
No part of this document may be reproduced or transmitted in any form or by any means without the prior written consent of Huawei Technologies Co., Ltd.

Leading New ICT  Building a Better Connected World

Safe City Extra