IDC Government Insights

A N A L Y S T C O N N E C T I O N

Alan Webber
Research Director

Next-Generation National Security and Public Safety in Europe

June 2016

As the threats and risks from cyber criminals, terrorists, gangs, nation states, and others continue to grow and evolve; national security and public safety officials in Europe face one of the most difficult challenges in government right now to keep citizens, cities, and nations safe. And often that means understanding the global cultural, social, and technological trends and adopting technologies that help them in reducing the threats and consequences of these trends. In addition, the European Union (EU) adds additional complexities for example with there being both national borders and EU borders, different travel regulations for EU member citizens then non-EU member citizens, and EU responses to immigration instead of national responses to immigration.

The following questions were posed by Cisco to Alan Webber, Research Director, IDC Government Insights, on behalf of Cisco's customers.

Q. What are the trends affecting national security and public safety in Europe?

A. Given the nature of Europe and the EU, there are a number of both direct and indirect cultural and social issues and trends that are affecting national security and public safety in Europe. The following trends are foremost:

- **Changing demographics.** Government services, and specifically national security and public safety agencies, will have to deal with these changes by increasing the types of services they offer, the way services are delivered, and technologies they employ to provide services for citizens. Some of the significant demographic trends include:
  - **Population growth.** The population of the world will continue to grow at a significant rate. IDC estimates that the population of the world will add more than 1.3 billion people to reach a population level of 8.5 billion by 2035, with much of the growth coming in developing countries.
  - **Median age increases.** People are continuing to live longer through better access to resources and medical care. The current global median age is approximately 29 years. By 2035, IDC estimates that the global median age will reach 35 years, with the median age for developed countries jumping to 45 years and the median age for developing countries jumping to 33 years.
  - **Migration patterns.** People move from location to location driven by opportunity, economics, war, starvation and other causes, often with little regard for national boundaries. IDC estimates that between 3 and 5% of the world's population currently live as migrants in countries other than their birth country. By 2035 Asia, Latin America and South America, and Africa will lose approximately 40 to 60 million people as North America, Europe, and Oceania will continue to gain.

- **Vulnerability of resources.** Clean water, food, energy, trees, minerals, and other resources are becoming more depleted and in higher demand. As developing nations continue to develop, the demands for resources will grow too. This will likely increase the level of conflict over these resources.

- **Urbanization.** IDC estimates that approximately 45-50% of the world's population currently lives in an urban area, with 80% of people in developed countries living in urban areas and 50% of people in developing countries. By 2035, as people continue to migrate, this number will rise to over 60%. The result will be that urban areas will be challenged to provide adequate resources and infrastructure.

- **Political stability trends.** Though there is always some instability across nations and regions, there are two instability issues that affect national security and public safety in Europe – the crises in North Africa and the Middle East and the crises within the EU itself. There are other issues, such as the redevelopment and rearmament of Russia, but these two are the largest ones at this point.
    - **North Africa and the Middle East.** Most pressing right now is the instability in the Middle East and North Africa. Events in Libya, Egypt, Algeria, Sudan, Syria, Lebanon, and Mali have demonstrated that pressing economic issues have led to instability and regime change along with the rise of radical groups.
    - **EU stability.** The stability of the EU itself is in question as Britain debates whether or not to remain a part of the EU. The question is what will the impact be on economic stability in Britain and the EU, travel and free movement of people (including immigration and refugees), and security cooperation.

- **Migration and refugees.** Immigration and refugees have been a consistent concern for European nations. The instability in North Africa and the Middle East has resulted in a new wave of refugees leaving their homes for the relative safety and better economic opportunities of Europe, Turkey, and elsewhere. An additional issue for is that there may be people connected to terrorist groups or criminal gangs hidden among the refugees.

Q. What are the current primary national security and public safety issues facing Europe?

A. There are new threats emerging specific to the national security and public safety space every day. The current trends that national security and public safety professionals in Europe need to be aware of include:

- **Border security.** Within both the nations of Europe and also the European Union, there are significant concerns with effective securing borders and border security that are tied to immigration and refugees, terrorism, smuggling, and other crimes. For example, in 2015 over 1.3 million refugees applied for asylum in Europe, with a significant majority coming from war-torn Syria. This is an increase from approximately 280,000 individuals coming into Europe in 2014.

- **Crime and terrorism.** Law enforcement and public security efforts in Europe have done well with combatting and reducing traditional forms of crime. Major crime categories in Europe including homicide, robbery, assault, burglary, and theft have stayed stable or dropped between 2008 and 2013 (the last available data from Eurostat). Since 2005, 292 people have been killed and over 890 wounded or injured by terrorists and during terrorism attacks. Closely related is Islamic radicalization. The terrorist attacks in Paris and in Brussels were carried out by perpetrators who were EU citizens, but had become radicalized while in Europe, left for the Middle East, then returned to Europe to carry out the attacks. Understanding, tracking, and countering these factors are key efforts among agencies to reduce the radicalization of European immigrants from Muslim countries.

- **Cybercrime and digital security.** Cybercrime is one of the largest threats that national security and public safety agencies must face. IDC has estimated that in 2015 alone there were over 82.5 million cyber-attacks globally resulting in approximately $625B in losses. Cybercrimes include a broad range of offenses and dangers that range from IP theft to espionage, malware to ransomware, financial theft to cyber terrorism, and more. Cybercriminals range from lone individuals, to small loosely connected groups, to organized enterprises and nation states. Because of the nature of computer networks, cybercrimes are often a cross-border activity with cybercriminals and nation states attacking targets in in other countries, complicating the investigation and any prosecution or other response.

- **National Security and Defense collaboration.** One of the more interesting trends has been the increase in collaboration between National Security and Defense resources on the National theatre. This collaboration is often a result of a lack of resources or specialized knowledge is specific areas such as counter-terrorism, explosives identification and neutralization, weapons of mass destruction, aspects of organized crime, and others. How to make this work without making the military into the police or the police into the military is a key question many nations are struggling with.

Q. What are the key topics in border security for Europe?

A. Border security is a unique issue within the EU. Individual nations are responsible for securing their own borders within the context of the Treaty of Lisbon that allows for free movement of people and goods within the EU. These same nations, and especially those with external facing borders, are responsible for securing and controlling entry into the EU. Within this context the primary issues are:

- **Border crossing and entry points.** The EU is composed of 28 countries and six candidate countries that share boarders with 20 other countries along 13,454 KM of land borders and almost 66,000 KM of coastal borders, making it difficult to secure every possible entry point. Besides managing the actual border crossings and entry points, national security officials must also manage a significant number of people who are already within their borders but no longer allowed to stay.

- **Maritime border security.** The EU has over four times the KM of coastal borders as land borders including all of the northern Mediterranean Sea, the Black Sea, the Atlantic Ocean, and the Baltic Sea. Maritime borders have traditionally been more difficult to secure and monitor. Significant movements of goods and people, both legal and illegal, happen every day in ports across Europe. It is important to national security and public safety officials that these maritime borders be secured against numerous threats including human trafficking, drug, weapons, and other types of smuggling, terrorism, and even health threats such as Ebola, polio, and MERS.

- **Supply chain security.** Another major issue for Europe are threats to and from the supply chain. The EU imported over 1.7 trillion Euros in goods and exported almost the same in 2015 among trading partners including the U.S., China, Russia, Turkey, Japan, and South Korea. Most public safety efforts in this area are aimed at stopping the traditional criminal movement of goods and people including counterfeit goods, illegal goods, and others. Efforts by the EU to secure the supply chain include advanced notification of contents to the destination and pass through countries, screening and validating cargo and goods, securing cargo in transit, and increased inspection of cargo on entry. It also includes the credentialing and reviewing of those individuals who are involved in the process.

Q. What are the key topics in digital security for Europe?

A. Just as the number of traditional threats that Europe faces continue to grow and change, so do the technologies and models for protecting against them. The proliferation of digital technologies continues to add to complexity that national security and public safety officials must fight against in the following areas:

- **Digital access control.** The purpose of digital access control is to manage who has access to the data and information, what data and information they have access to, and when do they have access to it. Access can be controlled through credentials that include a number of mechanisms like identity-based, role-based, attribute-based, organization-based, rule-based, and others. Newer technologies and new applications of existing technologies such as digital rights management (DRM), encryption, and even block chain and ledgers are leading the effort to move the management of the access from the system level or the account level or even the document level down to the data level.

- **Critical infrastructure protection.** Critical infrastructure is the skeleton on which the modern country exists. The ability to access and cause significant damage to both people and systems through digitally attacking the infrastructure including transportation systems, utility and water systems, energy grids, and others is a very real threat that national security and public safety officials face. These infrastructure systems (including SCADA, ICS, and AIS systems) are composed of software and hardware from various vendors who often did not take security into account in their design and implementation. The result is that these systems are often vulnerable and damage to these systems could have wide ranging impacts.

- **Information protection and privacy.** Information protection and privacy efforts of citizens including the encryption of data for privacy purposes are key issues that national security and public safety professionals need to consider including what is the balance point between security and privacy. Technology always has two sides. The same modern technologies such as smartphones, tablets, laptops, wearables, encryption, and others that citizens use every day for personal purposes and to protect themselves from hackers and cybercrime can also be used for illegal purposes such as communicating about a crime or protecting illegal data from being spied on by a government.

- **Secure information sharing.** The world is interconnected, and the ability of EU, national, provincial, city, and private sector partners in national security and public safety to share timely and accurate information is essential. This includes many models of sharing including one-to-one, one-to-many, and many-to-many, and many-to-one. The technologies that provide this sharing range from fusion centers to incident command systems to portable handsets to mobile devices and more. But it also includes the systems and processes that ensure that the information and data can be shared with the appropriate people and roles, at the correct time, and in the way that makes it best available for them to use it.

Q. What are the associated technology trends for border security and digital security?

A. Technology is a primary factor for both the changes that national security and public safety agencies are going through and for the threats and challenges that they face. This is not a new trend. What's different, however, is the increasing rate of change and the speed at which security must be continually updated to the following areas:

- **Internet of Things (IoT).** The Internet of Things (IoT) and ubiquitous computing (or pushing the computing power to the edge of the network) are key technologies that national security and public safety officials need to be aware of. IoT technologies, including various forms of sensors and other devices that have the ability to use the internet to communicate with other enabled devices and systems. The devices can then be deployed in corrections situations, law enforcement operations, emergency response, and national security to shift data feeds from

being static to real time, place technology in places where people can't be either because of the environment or because of resource limitations, improve the ability to share information, and increase operational efficiency. Even though there are significant benefits from IoT, there are still issues such securing the data stream, protecting the integrity of the data, and putting appropriate policies in place.

- **Analytics and big data.** Closely tied to IoT are analytics and big data. Big data refers to large and complex data sets that traditional data processing techniques are not adequate or effective in deriving information and knowledge from. That is where advanced analytics comes in – employing unique analytics and analytical modeling including predictive modeling, threat analysis, risk analysis, event management, and other technologies to derive better and more relevant information from the data being collected.

- **Computing at the edge.** The current national security and public safety model requires that data collection, analysis, and decision making happen in centralized nodes. However, the amount of information now being generated at the edge through IoT, mobile devices, and more along with the increasing speed of threats will further push applications to the edge and require stronger links between the edge and nodes. Agencies and nations are addressing this through edge BPM, optimizing mobile broadband and LTE resources, and improving systems roaming.

- **Identity and trust model.** Phishing and spear phishing are digital versions of a very old game of identity fraud and identity theft. Though phishing and spear phishing are two commonly heard terms, the issues that national security and public safety agencies face is much larger. It is important that agencies know that who you are interacting with and is accessing your systems and data is who they say they are through identification, authentication, and authorization. Identification is the process of positively identifying a person or entity, authentication is confirming that identity with known information, and authorization is indicating which information and resources they should be granted access to.

- **Video technologies.** Video technologies have a range of roles in national security and public safety from surveillance and detection to video and photo enforcement to license plate recognition to personal and group communication. But video technologies don't operate independently. To drive value from video technologies requires supporting technologies such as networks and communication technologies, data storage technologies, analytics technologies, and others.

- **Mobile communications.** More content and more types of confidential and classified content are collected, communicated, accessed, and analyzed on mobile devices. The ability to have secure mobile communications, whether data, voice, and/or video, is critical for national security and public safety agencies. When agencies consider purchasing secure devices, or any mobile devices for that matter, they need to make sure that they have all of the foundational pieces in place. This includes ensuring that agencies employ Mobile Device Management (MDM) and Mobile Application Management (MAM) applications in place, ensuring devices have a trusted boot and runtime, user authentication, data encryption both in transit and at rest, and malware detection.

ABOUT THIS ANALYST

Alan Webber is Research Director for IDC Government Insights. In this role, Alan leads IDC's National Security and Intelligence research program as well as IDC's government cybersecurity and cybercrime research efforts. Specific areas of research interest for Alan are the national security and cybersecurity aspects of technology policy, cybercrime, big data and analytics, internet of things, 3D printing, automation, cognitive computing, encryption, digital risk and security, and privacy.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc-gi.com