IDC Government Insights

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

Alan Webber
Research Director

Scaling Public Safety and National Security in a Digital World

March 2016

As the threats and risks from cybercriminals, terrorists, gangs, nation-states, and others continue to grow and evolve, national security and public safety officials face one of the most difficult challenges in government right now to keep citizens, cities, and nations safe. Often that means understanding global cultural, social, and technological trends and adopting technologies that help reduce the threats and consequences associated with these trends.

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

Q. What are the global megatrends that will impact national security and public safety over the next 10 years?

A. A number of culturally and socially significant trends, separate from technology trends, are progressing in the world that either are affecting or will affect national security and public safety. These trends stretch from the empowerment of the individual through information and technology, to the shifting demographics of people and cultures, to threats through global climate change and resource vulnerabilities:

- **Empowerment of the individual.** Through technology, an individual has the ability to create more content than at any time before. That same individual also has more access to more information than at any time in history through the use of the Internet, computers, tablets, smartphones, and other technologies. The result is that individuals are more connected to the culture they live in, both at the local level and the global level, and can have a larger impact on other people, communities, and culture. Examples of this from a national security perspective range from a small group of Russian hackers employing ransomware against public institutions such as hospitals and utilities to using mobile devices, connected cameras, and other devices to collect, modify, and share appropriate and inappropriate content.

- **Changing demographics.** Changing demographics, or the changing distribution of the human population, is already producing a world that is different from the world our parents and grandparents knew, and it will be even more different from the world our children and grandchildren will know. The result will be that 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 they deliver services, and

the technologies they employ to provide services for citizens. Some of the significant demographic trends are:

- **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 because of better access to resources and medical care. The current global median age is approximately 29. IDC estimates that by 2035, the global median age will reach 35, with the median age for developed countries jumping to 45 and the median age for developing countries jumping to 33.
- **Migration patterns.** Since ancient times, people have been a migrant species moving from location to location driven by opportunity, economics, war, starvation, and other causes, often with little regard for national boundaries. IDC estimates that 3–5% 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, oil and energy, forests and trees, minerals, and other resources are becoming more vulnerable to misuse, short supply, or overcontrol. For example, driven by population increases, demand, and climate change, the number of people living in water-stressed or water-short areas is expected to be half the global population by 2035. At the same time, growing populations and increasing GDP are driving energy demands. As developing nations continue to push forward, the demands for energy from this growth will more than triple. The potential result is that some of these resources will be more difficult to obtain and if so will increase the level of conflict.

- **Climate change.** Closely related to the vulnerability of resources is global climate change. Climate change includes global warming, increasing CO2 levels, and threats to ecosystems that become national security issues when they affect human populations. Whether natural or manmade, global temperatures are expected to rise and thus impact sea levels by the melting of Artic icecaps and potentially increasing the number of significant weather events. The result is that national security and public safety officials need to be prepared for changes in shipping lanes, flooding of coastal areas, and increasing frequency of significant weather events like hurricanes and typhoons.

- **Urbanization.** IDC estimates that approximately 45–50% of the world's population currently lives in urban areas; 80% of people in developed countries and 50% of people in developing countries live in urban areas. 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 to support this increase while dealing with consequential issues, such as crime.

Q. What current trends do national security and public safety professionals need to be thinking about?

A. New threats and issues specific to the national security and public safety space are emerging almost every day. IDC recently spoke with a national security and public safety professional who commented, "Working in national security and public safety is very similar to the little Dutch boy trying to plug the holes in the dam with his fingers; the only difference is that there are already more holes than fingers, and new holes show up every day." Some of the current

©2016 IDC

trends that national security and public safety professionals need to be aware of are the growth in the number and breadth in cybercrimes, balancing security with information protection and privacy, and digital transformation of the security and safety role in conjunction with the digital transformation of the agency:

- **Cybercrime.** Cybercrime is one of the largest threats that national security and public safety agencies must face. Cybercrime is any crime or criminal act that includes the use of a computer or similar technology such as mobile phones and the Internet in the execution of the crime or where a computer or information technology system is the target. Cybercrimes include a broad range of offenses and dangers that range from IP theft to espionage, malware to ransomware, financial theft to cyberterrorism, and more. Cybercriminals range from lone individuals to small loosely connected groups to organized enterprises to 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, thus complicating the investigation and any prosecution or other response. IDC has estimated that in 2015 alone, over 82.5 million cyberattacks globally resulted in approximately $625 billion in losses. As technology becomes more and more culturally embedded, the types and number of cybercrimes will only continue to increase.

- **Information protection and privacy.** Though less of a direct issue, 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 be considering, including determining the balance point between security and privacy. Technology almost 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. Technology that can gather evidence and information that is potentially vital to an investigation can potentially make citizens more vulnerable to being hacked or worse.

- **Distributed threats.** Not every threat comes from a single source in this new world. Instead, because of the interconnected nature of our world, most threats come from multiple, distributed sources and can have multiple targets and multiple impacts. For example, distributed denial-of-service (DDoS) attacks take advantage of the distributed computing power of compromised systems to create a distributed system with the single goal of blocking or taking down a Web site or access to a network. Other examples include the use of malware to infect a computer system that is then used in a kinetic method to damage real-world machinery such as a manufacturing system or a water control and sanitation system.

- **Wearables and video.** Wearables that record information and video add a whole new dimension to national security and public safety. They provide often necessary information for law enforcement agencies and national security agencies by using body cameras, video surveillance cameras, microphone systems, and other technologies and sensors to collect the information. This information is matched up with analytics that are used to analyze the data and provide intelligence to the agency and in some cases accountability for the actions of officers and agents. These same devices can also improve accountability and provide additional information to the public.

- **Digital transformation of the agency.** With all of the new technology, national security and public safety agencies are on the brink of a digital transformation. The technologies employed by these agencies and the job functions and operations of the agencies themselves will change. For example, in an era of autonomous vehicles, there is less

need for traffic officers and highway patrol officers who are responsible for monitoring and managing vehicle traffic. This role may be replaced by code enforcement officers whose job it is to scan the computer code of autonomous vehicles, identify hacks and changes to the computer code such as a street racer might employ, and prosecute those future crimes. At the national security level, though conventional threats will not go away in the foreseeable future, the establishment of U.S. Cyber Command (USCYBERCOM) and other similar agencies is an indication of the shifting nature of the fight and will draw additional resources away from conventional agencies.

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

A. Technology is a primary factor both for 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 for either; for example, national security agencies had to deal with both the upsides and the downsides of the emergence of intelligence satellites and geospatial information, much like what law enforcement agencies went through with the introduction of radios and then laptop computers into patrol cars. The difference is in the rate of change, which is increasing, and the speed at which the opposition is adopting similar and counter technologies:

- **The Internet of Things (IoT) and ubiquitous computing.** The 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 include 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 static to real time, employ 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 associated with IoT and ubiquitous computing, there are still potential issues such as securing the data stream and protecting the integrity of the data and putting appropriate policies in place that both increase adoption and enhance regulatory and protective regimes.

- **Secure mobile communications.** As more content and more types of content are collected, communicated, accessed, and analyzed on mobile devices, in the national security and public safety space much of that content will at least be confidential and not for public distribution and some may be classified for investigative or national security reasons. Thus the ability to have secure mobile communications, whether data, voice, or video, is critical. 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 they employ mobile device management (MDM) and mobile application management (MAM) applications in place as well as ensuring that devices have a trusted boot and runtime, user authentication, data encryption both in transit and at rest, and malware detection.

- **Analytics and big data.** Closely tied to IoT are analytics and big data. Big data refers to the large and complex data sets, such as those gathered from multiple IoT devices and other sources, that traditional data processing techniques are not adequate or effective in deriving information and knowledge from. That is where advanced analytics comes in. Agencies are employing 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.

©2016 IDC

- **Identity and digital trust model.** Phishing and spear phishing are new digital versions of a very old game of identity fraud and identity theft. Though phishing and spear phishing are two commonly heard terms around identity, identity management, and trust, the issues that national security and public safety agencies face is much larger. It is important that individuals with whom you are interacting and who are accessing your systems and data can be verified to be who they say they are. Identification is the process of positively identifying a person or an entity, authentication is confirming that identity with known information, and authorization is indicating which information and resources that person or entity should be granted access to. This is critical in the national security and public safety space to control the access and release of classified information.

- **Social media.** Most national security agencies and public safety agencies have a Web page, a Facebook page, maybe a Twitter feed, and/or an Instagram account. Some may even use blogs or microblogs like Tumblr to communicate and educate the public about their mission, what it is they are doing, some of the technology they use, and even situations that are happening such as an Amber Alert. Using social media channels is a great way to communicate with an audience that is interested in what the agency is doing, but that is only half of the equation when it comes to social media.

- **Cloud and shared services.** Cloud technologies and shared services can help public safety agencies gain secure access to applications, communications, and resources easily. However, it is important that these services have the appropriate level of security and privacy assessments to mitigate concerns about hardware failure and data loss, data corruption and leakage, and insecure connections and interfaces.

Q. How can national security and public safety agencies drive the most value from their technology investments?

A. National security and public safety agencies have neither the time nor the budget flexibility to invest in technologies that they are not relatively certain will be beneficial in protecting against threats. To do this, beyond traditional budget justifications for the procurement of a new technology, agencies need to focus on whether the technology will increase efficiency in mission delivery and effectiveness, decrease legacy maintenance costs and the resultant training costs, be able to meet multiple mission needs, and function as a force multiplier for the agency:

- **Increase efficiency and effectiveness.** Primary decision criteria for the adoption of any technology by a government agency are whether or not the technology will increase efficiency and improve effectiveness. For new technologies, there will be a change effort and an adoption curve that can reduce or eliminate initial measures of efficiency and effectiveness, but over a relatively short period of time (less than a year) there should be positive indications of improved efficiency and effectiveness.

- **Decrease maintenance and training costs.** The adoption of any new technology often comes with a shift in maintenance costs and in costs to train employees in how to use the new technology as part of the change and implementation effort. The best scenario involves technologies that reduce maintenance costs because they are easier to maintain or they are upgraded automatically. At the same time, they should decrease user training time and costs through user interface design and building on known user knowledge sets.

- **Meet multiple mission needs.** Within an environment of a constrained budget and operational limitations, technologies need to be able to meet multiple mission needs. For example, mobile devices can and need to function in multiple roles, from phones to information access points, cameras to biometric scanners, and hard drives to body cameras. There is the need for redundancy that is unique to national security and public safety missions compared with other agencies and the private sector, but it is still better to have a technology that meets multiple mission needs and then redundancy based upon priority and likelihood than to have multiple single application technologies.
- **Force multiplier.** Similar to meeting multiple mission needs, technologies adopted also have to be a force multiplier. In the context of national security and public safety, this means that by adopting the technology, the agency is able to have the same effectiveness as a dramatically larger operation or force. For example, adoption of a new technology such as patrol cars in the 1920s by the New York City Police Department allowed the same number of officers to cover a much larger area than they had previously covered on foot and on horseback. In the national security space, the adoption of new technology such as high-performance computers allows intelligence agencies such as the National Security Agency or the British Government Communications Headquarters to increase the amount of signals data and information processed on a daily basis.

ABOUT THIS ANALYST

Alan E. Webber is National Security Research Director for IDC Government Insights. Specific areas of research interest for Alan include government-focused cybersecurity, physical security, biometrics, Internet of Things, digital risk, and privacy.

ABOUT THIS PUBLICATION

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC Government Insights, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC Government Insights content available in a wide range of formats for distribution by various companies. A license to distribute IDC Government Insights content does not imply endorsement of or opinion about the licensee.

COPYRIGHT AND RESTRICTIONS

Any IDC Government Insights information or reference to IDC Government Insights that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC Government Insights. For permission requests, contact the IDC Custom Solutions information line at 508-988-7610 or gms@idc.com. Translation and/or localization of this document requires an additional license from IDC Government Insights. For more information on IDC, visit www.idc.com. For more information on IDC Custom Solutions, visit http://www.idc.com/prodserv/custom_solutions/index.jsp.

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

©2016 IDC