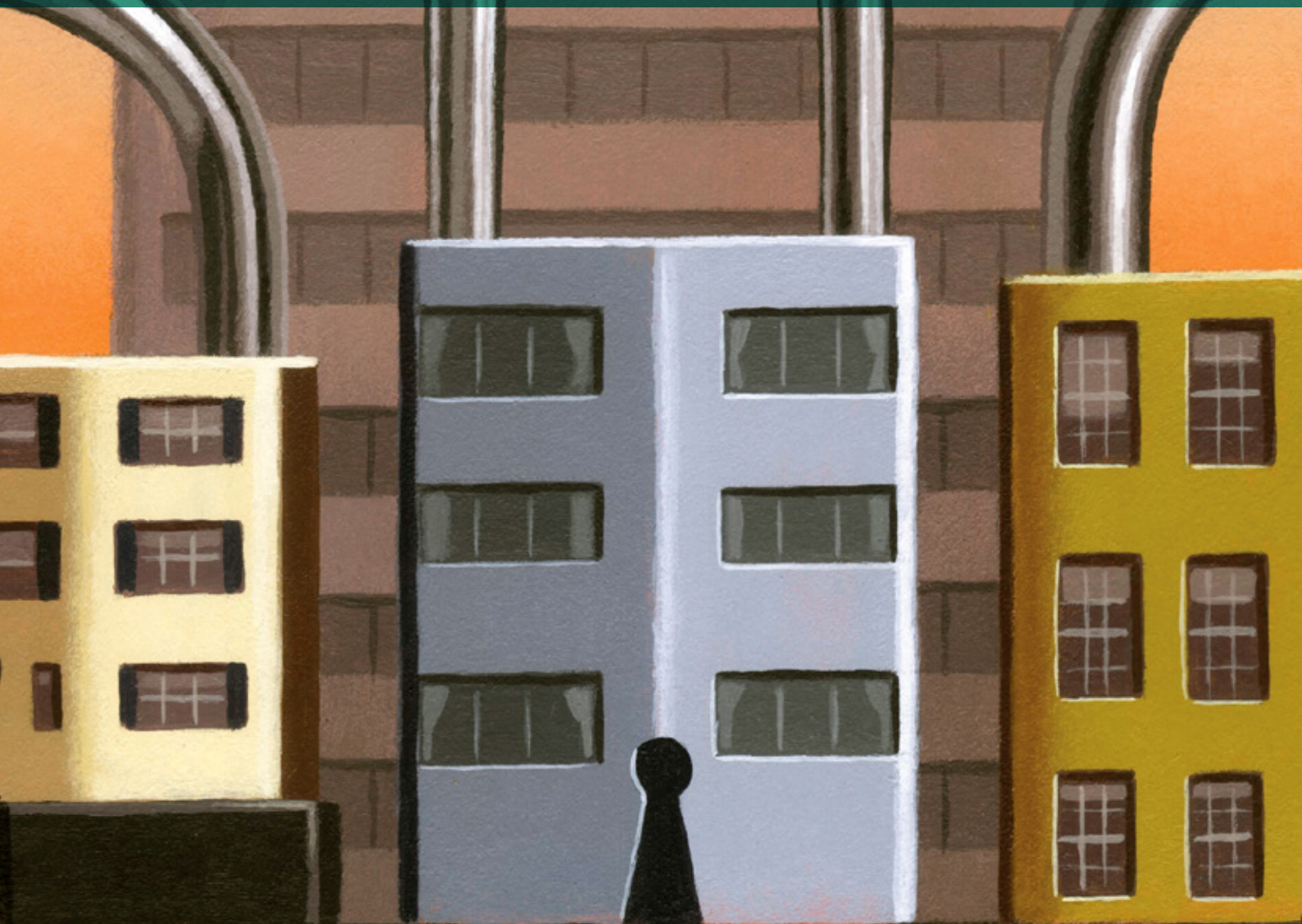


BCG

THE BOSTON CONSULTING GROUP

# How Technology and Collaboration Can Help Create Smart *and* Safe Cities



The Boston Consulting Group (BCG) is a global management consulting firm and the world's leading advisor on business strategy. We partner with clients from the private, public, and not-for-profit sectors in all regions to identify their highest-value opportunities, address their most critical challenges, and transform their enterprises. Our customized approach combines deep insight into the dynamics of companies and markets with close collaboration at all levels of the client organization. This ensures that our clients achieve sustainable competitive advantage, build more capable organizations, and secure lasting results. Founded in 1963, BCG is a private company with 85 offices in 48 countries. For more information, please visit [bcg.com](https://www.bcg.com).



THE BOSTON CONSULTING GROUP

# How Technology and Collaboration Can Help Create Smart *and* Safe Cities

**Agnès Audier, Michel Frédeau, and Sylvain Brun**

May 2017

## AT A GLANCE

---

Public- and private-sector leaders must move aggressively to prepare for terror and cyberthreats. As part of this effort, it is imperative to advance from the idealistic vision of a “smart” city that is vulnerable to a realistic vision of a smart and safe city. BCG has developed a set of recommendations that address the common challenges across an array of strategic, technical, and operational topics.

### **DEFINE A UNIFIED STRATEGIC VISION**

A diverse set of stakeholders—including government agencies, defense forces, and public and private security forces—need a unified strategic vision for security designed on the basis of a shared understanding of the main threats. This vision is essential for prioritizing objectives; guiding private-sector R&D and investment decisions; determining the requisite human, financial, and technological resources; and clarifying each stakeholder’s responsibilities.

### **PROMOTE ENHANCEMENTS TO TECHNOLOGY AND COLLABORATION**

Governments should encourage cooperation among all stakeholders. Cooperation encompasses clarifying standards and purchasing processes for technology companies that are developing security solutions, as well as enabling citizens to take a more active role in security.

---



**A**ROUND THE WORLD, PUBLIC-SECTOR leaders face the imperative to protect their cities from the rising threat of terrorism and cyberattacks. Since 2000, the number of terror attacks worldwide each year has increased sevenfold, and the number of victims has increased ninefold. Major cities, including Berlin, Brussels, London, Madrid, New York, and Paris, have experienced terror attacks that claimed many lives. Cyberattacks have also risen sharply, nearly 75% targeting public-sector systems.

The heightened threat level comes at a time when many countries have made significant investments in the creation of “smart” cities with advanced infrastructure and easy access to public data. They have also sought to raise their cities’ international profiles and promote infrastructure development by hosting large-scale events. Such efforts to increase comfort, convenience, and openness have had the unintended consequence of making cities more vulnerable to terrorism and cyberattacks. Furthermore, some countries, plagued by high crime rates in their large cities, must deal with additional strain on their security resources.

Although for all countries, urban security is a top priority, each country is unique in terms of its degree of focus and level of spending on public safety. To date, the US, the UK, and Australia have spent the most per capita annually. France, Germany, Italy, Spain, and Japan have spent significantly less. As countries continue to assess their risks and consider the appropriate level and allocation of resources, they must involve a diverse set of stakeholders and make decisions on a wide array of topics. For example, technology companies that are developing new solutions to enhance urban security need a clear understanding of technical standards, markets, and purchasing processes. In providing this clarity, governments can support technology companies’ R&D efforts.

To help leaders improve collaboration and decision-making processes, The Boston Consulting Group has conducted extensive research into determining the factors that enhance cities’ ability to protect themselves. We drew upon the best practices of countries at the forefront in addressing urban security, as well as other sectors facing similar challenges. We found that in seeking to protect their cities, all countries face a common set of strategic, technical, and operational challenges. In this report, we offer recommendations relating to each of these challenges.

Let us stress that we are not experts on security and antiterrorism initiatives. Rather, we seek to apply our in-depth understanding of public-sector decision-making processes and our global industrial experience to provide public- and private-sector leaders with a framework for addressing the challenges of urban security.

---

In seeking to protect their cities, all countries face a common set of strategic, technical, and operational challenges.

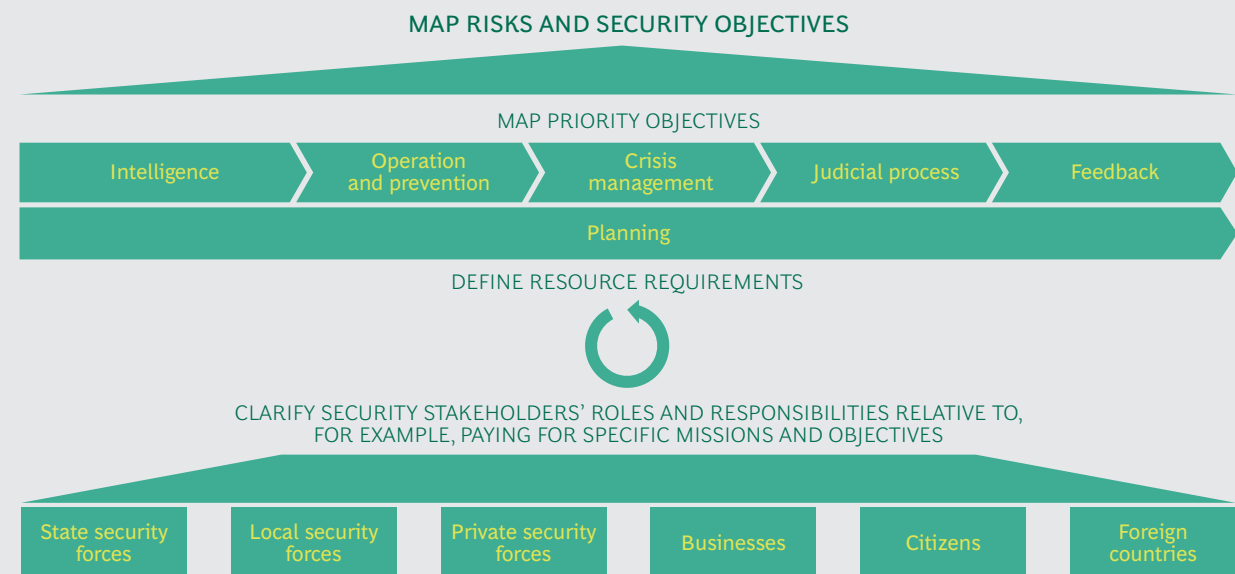
## Define a Unified Strategic Vision

A diverse group of stakeholders—including national, state, and local governments; police and other emergency services; transportation agencies; military forces; private security services; businesses; and citizens—are involved in protecting cities. To collaborate effectively and allocate resources to the right entities and in support of the right objectives, these stakeholders need to be guided by a unified strategic vision. In our discussions with public-sector leaders, we have found that such a vision has rarely been defined for the security ecosystem.

The national government should assign responsibility to an entity at the national level, as well as to entities at the appropriate local levels, for defining and regularly updating a unified strategic vision and discussing the related resource allocation. Such entities are commonly created to define and update strategies in the defense sector.

The entities should define the vision by identifying the main risks and threats and the objectives of enhancing security. (See Exhibit 1.) They apply this vision to prioritizing objectives and clarifying the main stakeholders' responsibilities relative to, for example, intelligence gathering and crisis management. Planning must occur across each of these dimensions. The entities should then provide initial guidance on the human, financial, and technological resources required to achieve these objectives. The stakeholders, in accordance with their authority, negotiate with the national or local governments on the resources allocated to help them meet their objectives. To gain insights into concerns such as technical requirements, entities would do well to engage in discussions with their counterparts in other countries. And because they must adapt to ever-changing threats, the entities should continually update the strategic vision on the basis of developments and adjust the objectives, resources, and responsibilities as necessary.

### EXHIBIT 1 | Defining a Unified Vision for Urban Security



Source: BCG analysis.

## Work with Technology Companies to Develop Effective Solutions

The public sector needs to foster a business environment that encourages technology companies to invest in R&D related to security technologies. Today, numerous obstacles confront companies seeking to serve the security technology market. Purchasing is fragmented among regional and local stakeholders (both public and private), each making relatively small investments. Furthermore, governments have not set clear priorities regarding the solutions they want. The absence of interoperability standards also impedes the adoption of solutions. Moreover, because governments tend to purchase proven solutions, startups with innovative technologies struggle to break into the market or lack adequate funding. For their part, many governments lack a clear view into the products and services offered by the security technology industry, while many security companies are not prepared to engage in in-depth discussion of the value of their offerings, relying solely on a general presentation of references.

To promote the availability of more effective solutions, governments should act on three related imperatives: developing expertise at the national level to support public stakeholders, setting technology priorities, and creating economic incentives and pushing for multipurpose solutions.

**Develop expertise at the national level to support public stakeholders.** At a minimum, national governments should help local authorities and public agencies define their technical requirements. But to provide more than basic support, a government could assume the role of the chief technology officer (CTO) for public stakeholders, by, for example, creating norms or labels for specific technologies and offering advice on the capabilities to acquire. The most expansive role for a government would be to act as a procurement agency that buys equipment and services for public—and possibly private—security-related entities in order to benefit from the scale effects of consolidated spending.

Defense procurement can serve as a model for governments' role in procuring security technologies. In some countries, a dedicated organization of the defense ministry is in charge of armament procurement and R&D and acts as a CTO by providing guidance to the entire defense industry. It also identifies and evaluates defense companies and technologies, defines norms, and certifies technology solutions.

**Set technology priorities.** To further support procurement, national governments should help cities identify the priorities for security technology investments. This effort begins by mapping the various available technologies to the main security-related activities. (See Exhibit 2.)

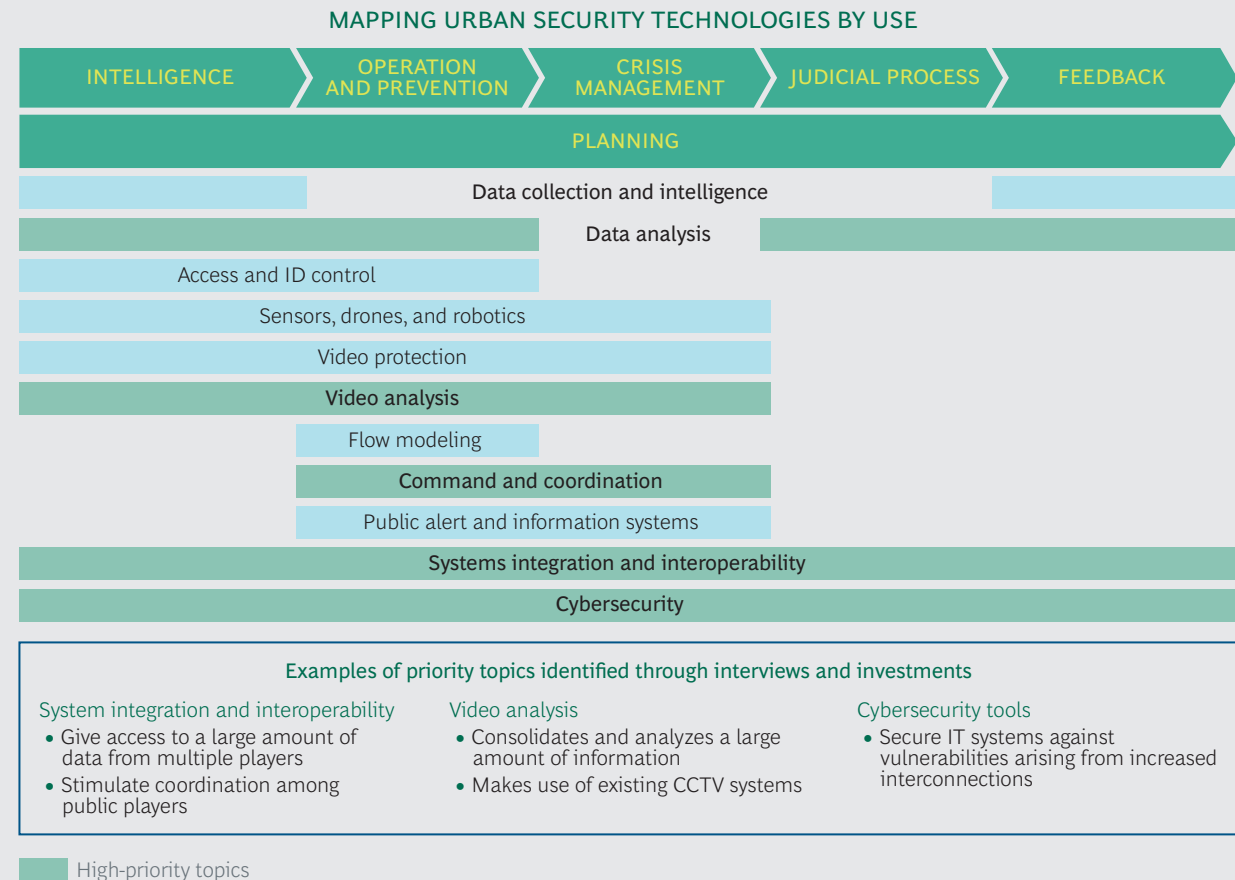
Examples from around the world illustrate the kinds of priorities governments are setting:

- The integration and interoperability of security systems have become major focuses of attention. For example, Mexico City, through its *Ciudad Segura*, or Safe City, initiative, is implementing a unified command-and-control center for all security forces (approximately 80,000 people), procuring high-tech equipment,

---

The public sector needs to foster a business environment that encourages technology companies to invest in R&D related to security technologies.

## EXHIBIT 2 | Mapping Security Technologies to Objectives



**Source:** BCG analysis.

**Note:** CCTV = closed circuit television.

sharing data across all public entities, instituting a monitoring and planning system for security forces, and establishing a dedicated training center.

- The analysis of video images has gained importance as technology solutions enable governments to consolidate and analyze a large amount of information captured by closed-circuit television (CCTV) systems. And data analysis has emerged as a priority in many countries, including Brazil, France, Israel, and the UK.
- Investments in cybersecurity are climbing as governments strive to protect the vast web of interconnected public and private IT systems in the smart city. Two types of cybersecurity solutions are required: perimeter protection systems that strengthen access barriers to IT systems and anomaly detection systems that identify and respond to unexpected activity.

**Create economic incentives and push for multipurpose solutions.** To promote innovations in security technologies, public stakeholders should establish economic



models and incentives that are both appropriate and effective. Some innovative economic models encourage the multipurpose use of technologies. For example, in London, CCTV systems installed for security surveillance are used also to investigate fraud and corruption. The utilization fees make it possible to accelerate the amortization of the systems' initial cost.

Governments are creating economic incentives for business development and innovation, by, for example, funding investment programs, increasing the visibility of requests for proposals, and providing tax advantages. For instance, the EU has launched Horizon 2020, an investment program that makes €80 billion available for research and innovation. The program aims to remove barriers to innovation and make it easier for the public and private sectors to work together. France has created “competitive clusters” that bring together companies and research and education organizations, including entities within the security sector, to collaborate on shared objectives.

The coordination among participants in the health and pharmaceutical industries provides a model for the security sector. For example, some governments encourage partnerships between large pharma manufacturers and public laboratories and have supported the development of a long-term vision for the use of technology in the health care system. National agencies also coordinate medical research, including the allocation of funding, and seek to stimulate innovation.

## Enhance the Security Network and Improve Cooperation

All countries must take steps to enhance their security networks and encourage cooperation among stakeholders.

**Involve more stakeholders and foster network collaboration.** To respond to rising threat levels, governments must involve more stakeholders—such as private security companies, businesses, and citizens—in the security network. They must also promote collaboration among these stakeholders through information sharing, integrated tools (notably, to support command and control), incentives, and clearly defined roles.



To achieve the objectives of a denser and more effective security network, governments need to apply innovative approaches to organization design. Most security networks still rely on rigid hierarchical and centralized organizations in which the chain of command starts at the national level and reaches down to other participants in the security network. Such an organization structure can hinder information sharing and cooperation, and in the event of an attack, communication linkages among participants can easily be disrupted.

To overcome the limitations of the hierarchical model, governments should consider implementing a decentralized, collaborative organization design known as *hyperarchy*. (See Exhibit 3.) Recent decades have seen several prominent examples of the hyperarchy model. In the private sector, well-known disrupters, such as Wikipedia and eBay, have achieved success by using shared norms and objectives to promote collaboration among dispersed participants in an informal network. Some terrorist

---

Governments must involve more stakeholders—such as private security companies, businesses, and citizens—in the security network.

### EXHIBIT 3 | The Hyperarchy Model Promotes Collaboration in a Dispersed Organization

|                               | <br>HIERARCHY  | <br>HYPERARCHY   |
|-------------------------------|---|---|
| Organization form             | Hierarchical and centralized top-down system  | Polycentric network of small, dispersed, and semiautonomous units   |
| Governance                    | Highly centralized authority; easily disrupted leadership   | Devolved authority; ability to resist when leadership is targeted   |
| Strategy                      | Uniform strategy and tactics across the network; little adaptability  | Decentralized tactics and action plans based on a common strategy; enhanced flexibility   |
| Alignment                     | Alignment through command and control   | Alignment through shared doctrine, norms, and objectives  |
| Boundaries and integration    | Static boundaries; complex integration of additional players  | Evolving and variable boundaries that facilitate integration (for example, with civilians and allies)   |
| Cooperation                   | Limited cooperation; siloed stakeholders interacting in a chain of command  | Naturally emerging cooperation; no formally specified relationship; patterns of reciprocity and reputation  |
| Information and communication | Closed architecture; segmented information  | Open architecture; networked information; interoperability with a collaborative platform  |
| Examples                      | <ul style="list-style-type: none"> <li>• Encyclopedias</li> <li>• Big technology companies</li> <li>• Major music and movie companies</li> <li>• Traditional retailers</li> <li>• Traditional threats to national security</li> </ul> | <ul style="list-style-type: none"> <li>• Wikipedia</li> <li>• Silicon Valley</li> <li>• Peer-to-peer platforms (for example, The Pirate Bay)</li> <li>• eBay</li> <li>• Terrorist organizations (for example, Al Qaeda and ISIS)</li> </ul> |

Sources: US Army War College; BCG analysis.

organizations have adopted a similar model to expand their reach and increase their agility.

To apply hyperarchy concepts to their organization design, security networks should decentralize and devolve power to their dispersed stakeholders. Capturing the benefits of resilience, agility, and innovation will require strengthening the connections among stakeholders, mapping interdependencies in order to clarify roles and responsibilities, and implementing new technologies to catalyze change and cooperation.

The role of private security forces is especially critical in defining a decentralized security network. In Israel, for example, private security forces are responsible for control of sensitive locations, such as the main airport and train station, while police and national security forces lead antiterrorism initiatives and the army manages border control. New York City has established a partnership between the police department and private security companies that promotes information sharing, provides alerts during crises and incidents, and offers jointly held training programs.

Governments must enhance businesses' involvement in the security network by conveying best practices and sharing video surveillance and other equipment. They must also increase citizens' involvement in the security network, as we discuss below.

At the same time that governments enhance their security networks, they must take steps to improve stakeholder collaboration, especially through the use of technology and access to tools held in common. Digital solutions can be used to align ways of working and to integrate IT systems. Paris is integrating access to surveillance videos from cameras located in streets, transportation networks, and tourist attractions, making these images available to all participants in the security network. Similarly, New York City has established a system that provides integrated access to surveillance videos (including from private cameras) and sensor data, along with real-time threat alerts. The EU has created an integrated database for tracking airline passengers' travels; the data is transmitted to all public stakeholders fighting terrorism.

Governments should also convene collaborative working groups of leading security players to provide a forum for discussing security topics. In France, the Secretariat-General for Defense and National Security has brought together transportation operators and the security managers of designated "entities of vital importance" to discuss security topics.

**Define a doctrine of use and regulate security services.** Governments should define a "doctrine of use" for both public and private security services that codifies their specific responsibilities, including when and how they can use force.

Governments can also empower private security services by establishing a regulatory agency, creating industry norms, or providing accreditations. Australia, Canada, South Africa, the UK, and the US have taken the lead in regulating private security services. For example, the UK has established the Security Industry Authority to regulate its booming private-security industry, which has grown at five times the rate of the rest of the national economy since 2010.

For models of how to prepare for and respond to urban security threats, governments can look to safety practices that are already engrained in everyday life, such as fire evacuation drills. Emergency plans to protect populations near nuclear sites can serve as models for developing more advanced approaches to security planning. For example, the French government has established comprehensive emergency plans to ensure safety at nuclear plants. The plans clarify incident procedures, including roles and responsibilities of the state and local governments and the site operator, the alert threshold, the information to be provided to the public, and the coordination of resources.

**Assign citizens an active role.** Promoting the greater involvement of citizens is essential. Among the most ambitious approaches is the creation of a program that has citizens act as "security reservists." In the event of a terrorist threat or attack, these reservists, typically retired police officers or security guards, are called to active service in support of full-time security forces. For example, reservists can provide additional security at airports during periods of heightened threat levels.

---

Governments should enhance businesses' involvement in the security network by conveying best practices and sharing video surveillance and other equipment.

To make the necessary changes to legal and regulatory frameworks, governments must reassure citizens that their freedom is being protected along with their safety.

Governments can encourage businesses to hire security reservists by providing accreditation of reservists' leadership and management skills and, more generally, communicating the benefits of employing a trained reservist. For example, in the UK, the Royal Air Force's Standard Learning Credit program helps civilians acquire valuable employment skills, including a positive work ethic, confidence, leadership and communication skills, and the ability to work under pressure.

Several countries have created programs that help citizens get involved in security on a local level, such as by participating in neighborhood surveillance. For example, Singapore has established the Vehicles on Watch program, in which citizens voluntarily place cameras in their cars to help improve security in streets and parking areas. In the US, Citizen Corps, operated by the Department of Homeland Security, trains citizens to assist in the recovery from a disaster or terrorist attack.

**Promote the public's acceptance of heightened security.** In many nations, the heightened security required to respond to terror and cyberthreats conflicts with existing norms and ethical safeguards relating to civil liberties and privacy. In some cases, laws and regulations that protect personal data and privacy limit the use of, for example, facial-recognition technology and phone records or place other restrictions on the actions of security forces. Although the tension between civil liberties and security is not new, it needs to be addressed within today's context.

In order to make the necessary changes to legal and regulatory frameworks, governments must reassure citizens that their freedom is being protected along with their safety. To accomplish this, governments should launch public debate and assess public opinion on key security topics, including the objectives and levels of security and the safeguards that protect civil liberties. Some cities have established ethics committees, forums through which government officials and citizens can discuss the need for heightened security and the civil-liberty tradeoffs.

**T**HE IMPERATIVE TO evolve from the idealistic vision of a smart city to the realistic vision of a smart and safe city is clear to the majority of leaders in the public and private sectors as well as to ordinary citizens. Indeed, the objective of making "cities inclusive, safe, resilient and sustainable" is among the United Nations' "17 goals to transform our world."<sup>1</sup> The challenge is how to make this happen. To start, governments should bring together the key stakeholders and ensure that the right expertise and insights are available to inform decision making. Before delving into the technical and operational details, it is essential to guide the effort by agreeing on a unified strategic vision for security. With this vision in place, stakeholders can begin the work of achieving a prosperous and secure future for their cities.

#### NOTE

1. See United Nations, "Sustainable Development Goals: 17 Goals to Transform Our World," January 2016, <http://www.un.org/sustainabledevelopment/development-agenda/>.

## About the Authors

**Agnès Audier** is a partner and managing director in the Paris office of The Boston Consulting Group and a core member of the Public Sector, Industrial Goods, and Strategy practices. You may contact her by email at [audier.agnes@bcg.com](mailto:audier.agnes@bcg.com).

**Michel Frédeau** is a senior partner and managing director in the firm's Paris office and a core member of the Energy and Industrial Goods practices. You may contact him by email at [fredeau.michel@bcg.com](mailto:fredeau.michel@bcg.com).

**Sylvain Brun** is a project leader in BCG's Paris office. He has extensive experience in the public sector and industrial goods topics. You may contact him by email at [brun.sylvain@bcg.com](mailto:brun.sylvain@bcg.com).

## Acknowledgments

The authors thank the government and corporate leaders they interviewed for their valuable contributions to this report. They also thank the following BCG partners and senior advisors, who participated in interviews or provided relevant contacts: Jeffrey Chua, Filiep Deforche, Philip Evans, Alastair Flanagan, Greg Mallory, Yves Morieux, Max Pulido, and Heinrich Rentmeister. Additionally, the authors thank Maud Guerlain, François Triclin, and Rodolphe Chevalier for their contributions. Finally, they thank David Klein for his writing assistance, as well as other members of the editorial and production team, including Katherine Andrews, Gary Callahan, Elyse Friedman, Kim Friedman, Abby Garland, and Sara Strassenreiter.

## For Further Contact

If you would like to discuss this report, please contact one of the authors.



To find the latest BCG content and register to receive e-alerts on this topic or others, please visit [bcgperspectives.com](http://bcgperspectives.com).

Follow [bcg.perspectives](#) on Facebook and Twitter.

© The Boston Consulting Group, Inc. 2017. All rights reserved.  
5/17



# BCG

THE BOSTON CONSULTING GROUP

Abu Dhabi  
Amsterdam  
Athens  
Atlanta  
Auckland  
Bangkok  
Barcelona  
Beijing  
Berlin  
Bogotá  
Boston  
Brussels  
Budapest  
Buenos Aires  
Calgary  
Canberra  
Casablanca  
Chennai

Chicago  
Cologne  
Copenhagen  
Dallas  
Denver  
Detroit  
Dubai  
Düsseldorf  
Frankfurt  
Geneva  
Hamburg  
Helsinki  
Ho Chi Minh City  
Hong Kong  
Houston  
Istanbul  
Jakarta  
Johannesburg

Kiev  
Kuala Lumpur  
Lagos  
Lima  
Lisbon  
London  
Los Angeles  
Luanda  
Madrid  
Melbourne  
Mexico City  
Miami  
Milan  
Minneapolis  
Monterrey  
Montréal  
Moscow  
Mumbai

Munich  
Nagoya  
New Delhi  
New Jersey  
New York  
Oslo  
Paris  
Perth  
Philadelphia  
Prague  
Rio de Janeiro  
Riyadh  
Rome  
San Francisco  
Santiago  
São Paulo  
Seattle  
Seoul

Shanghai  
Singapore  
Stockholm  
Stuttgart  
Sydney  
Taipei  
Tel Aviv  
Tokyo  
Toronto  
Vienna  
Warsaw  
Washington  
Zurich

[bcg.com](http://bcg.com)