RAND CORPORATION

Perspective

Expert insights on a timely policy issue

A Rapidly Changing Urban Environment

How Commercial Technologies Can Affect Military Intelligence Operations

William Young and David Stebbins

Police in an underdeveloped country beat a man to death in an alley after a political protest. A passerby captures the action on the video camera in his cell phone and sends it to a local television station, which broadcasts the action the same day. Minutes later the graphic video goes viral on the Internet. The government is immediately forced to confront a problem that either would have gone unnoticed in the past or would have been buried by the country's security apparatus and soon forgotten out of fear of reprisals from the authorities.

***

In the midst of civil war in another underdeveloped country, a young child uses a cell phone camera to photograph and geolocate snipers who are trying to protect the regime from rebel advances in the capital city. She sends the photos and geolocational data to rebel leaders, who confirm the snipers' locations and then attack them.

***

Hotel security cameras capture the faces of several assassins in a hotel in a large, first-world city. Using deep-web search capabilities, link-analysis tools, and facial-recognition software, the government is able to reconstruct the operation and identify the operatives, whose identities are then exposed on television and the Internet. Because they were unaware of the threat the cameras and related search technologies posed to their operation, the future travel and utility of these operatives is now in question.

These three brief composite examples show how several commonplace commercial technologies can be combined and used in unique ways to reshape an urban environment[1] and to disrupt how we live and work at home and abroad. The technologies are not new but are becoming ubiquitous and are being used in new ways.[2] They highlight a democratizing trend that gives more people the freedom and power to use any number of new, commercially available technologies to innovate and to challenge existing government rules and community practices.[3] This democratizing trend, however, comes at a cost to privacy, security,

Anyone with a smart phone can now be a news reporter, a detective, and a spy.

and secrecy and is changing the way people interact socially and politically. It is changing the way we conduct business, diplomacy, intelligence operations, and war, the future of which is likely to be increasingly urban in nature.[4]

All of the commercial technologies we are about to discuss can be used to identify and track individuals and to discern patterns in their behavior over time.[5] They are persistent and are dual-use, which means that they can benefit society or harm it. Although they are intended for commercial purposes, such as learning about shoppers' preferences and finding new markets, they can easily be used by police and security services to identify and track criminals, terrorists, insurgents, and spies. This means that these technologies have the potential to disrupt military intelligence operations and to jeopardize the plans, actions, and security of the warfighter.[6] In turn, the intelligence officer, the warfighter, and others who often live and work on the margins and in the gaps of society can use many of these same technologies to skirt government control, as well as to enhance the effectiveness of their operations. The nature of these human activities remains the same, but the infrastructure and urban setting in which the activities occur and in which many future wars will be conducted are changing in ways that may be hard to realize. Some of the most disruptive technologies in this rapidly changing environment are also the most common.[7] The key lies in understanding what they are and how they can be used in the next five to ten years to protect and otherwise aid military intelligence collection and the warfighter.

Mobile Communication

Anyone with a smart phone can now be a news reporter, a detective, and a spy. The handheld phone is becoming as ubiquitous in the third world as it is in the first world. It provides its owner with Internet access, video and photography, and GPS tracking, along with applications for various analytics. The location and movement of a phone across an urban landscape can be determined easily by the communications towers it uses.[8] It also can be turned into a receiver/transmitter. The phone itself enables instant, widespread mobile communication but, when coupled with other technologies, such as facial recognition and pattern recognition software, predictive analytics, deep-web search capabilities, and link analysis tools, it becomes perhaps the single most significant threat to privacy, secrecy, and security. The dangers to clandestine collection are myriad.

Having a cell phone means that an intelligence officer can be tracked. Not having one, however, is equally alerting. After all, who doesn't have a cell phone, and why would it be left at home or turned off at regular intervals during the day or in the course of a week? Behavior of this type is a way of identifying anomalies and patterns that might be worth further investigation. Being able to blend into the landscape is an essential feature of clandestine intelligence operations—one made considerably more complex by this everyday, everywhere technology. The ubiquitous nature of these new handheld devices means that case officers need to be increasingly aware of where and how this technology can be used against them, as well as how they might be able to use this particular technology to their advantage. Multiple layers of obfuscation and VPN nesting, for example, under the right circumstances, could provide security for conversations that otherwise would be open to track-

ing.[9] Even just being more aware of what is possible in terms of the threat will be a necessary input to operational planning.

The trends are for this technology to become smaller, lighter, and cheaper and to continue growing in diversity and spread of use. Some of the newest applications are for monitoring health and other biometrics and diagnostics, as well as for virtual gaming, data sharing, and information searches. Additionally, the technology's form is changing from something that is handheld to something that can be wireless and worn, as eyeglasses or on the wrist, or embedded in clothing in the future. What is perhaps most significant is how the technology can become a platform for other applications and for collecting and analyzing data and events—such as assessing mass protests and other large events in real time by using crowd-sourced reporting techniques.[10]

Ambient Sensing

Ambient sensing describes the persistent ability to use a given infrastructure to identify and track individuals and things within a sensor-heavy environment, such as a city or a network. This ability has also been called *ambient findability*.[11] The following paragraphs review some of the most common commercially available technologies currently being used.

GPS

The use of GPS tracking as a technology has become widespread and is open to abuse by individuals, governments, and businesses. It can be found in an ever-widening range of products. One of the most startling developments in recent years was a magnetic business card displayed by a Chinese vendor at the Las Vegas Electronics Show in 2009. He explained that the card contained a GPS tracking device and could be slapped on the bottom of a vehicle to keep track of a business partner or unfaithful spouse. Rental car companies often have at least one GPS device on their cars to ensure compliance with the distance and range stipulations of the rental contract. Foreign intelligence services can also easily embed similar devices on the vehicles of diplomats and businesses to establish patterns of behavior and contacts with country nationals.[12] Countermeasures engineered to spoof these systems may function well technically but are unlikely to produce the desired results if the police or host intelligence service couples the GPS tracking with physical surveillance and cameras. Jamming the devices will send them a clear signal that you are in fact something more than you pretend to be. Other technical attempts to fool these systems could have the unintended effect of exposing what the military case officer, warfighter, diplomat, or businessperson most wants to hide.

Radio Frequency Identification Devices

The use of Radio Frequency Identification (RFID) devices is becoming widespread. These sensors already are used to locate everything from rental cars in large parking lots to trauma equipment in hospitals.[13] Some construction workers put the devices on

Technical attempts to fool these systems could have the unintended effect of exposing what the military case officer, warfighter, diplomat, or businessperson most wants to hide.

their tools to ensure that they have what they need in their trucks before leaving home in the morning. RFIDs make finding things extremely efficient. Once they are included in clothing and monitored through the infrastructure of a city, they will make finding people equally efficient. This will be an immediate boon to businesses that want to identify shoppers as they pass certain stores on the street or specific displays inside. Combined with detailed web histories of a customer's past purchases, shop owners will be able to customize their sales offers. Police and security services, no doubt, will find similar uses for the technology, which, once embedded in driver's licenses, passports, and other documents and articles of clothing, can provide a foundation for logging, analyzing, and predicting an individual's movements and relationships over time and in real time. As part of a predictive policing effort, some police departments in the United States are already using scanners, along with RFIDs on license plates, to locate stolen vehicles.[14] A foreign security service could easily use the same techniques to determine the ownership of vehicles in areas that are otherwise off-limits to foreigners.

In war, a sensor-rich battlefield environment can cut two ways: providing the warfighters, collectors, and analysts with data previously unavailable and yet simultaneously creating an illusion of dominant knowledge of the enemy, who could take advantage of the same technology, data, and environment to mislead and disrupt through deception. At a minimum, the opportunities bring with them new challenges for both sides.[15]

In addition to the increasing ubiquity of these devices in cars, equipment, and clothing, the trends are for GPS, RFIDs, and other types of sensors to be used in conjunction with wireless mesh networks in cities and haptic technologies embedded under people's skin.[16] In sports medicine, *physiolytics* is the relatively new science and practice of linking wearable computing devices (watches and shoes) with data analysis and quantified feedback to improve performance.[17] Further advances in the general area of ubiquitous sensing include recent work on bendable "wallpaper" cameras (also called *flexible lens arrays*) that can wrap around lampposts and adhere to walls and other building structures, as well as automobiles, to monitor selected activities and to capture data that might otherwise go unnoticed.[18]

Biometrics

By identifying foreign fighters and terrorists who pose a threat to military operations and plans, the proliferation of biometric collection systems on the battlefield already has and will continue to yield significant intelligence and force protection results. In addition, facial recognition software, iris scans, and fingerprinting are

In war, a sensor-rich battlefield environment can cut two ways: providing the warfighters, collectors, and analysts with data previously unavailable and yet simultaneously creating an illusion of dominant knowledge of the enemy, who could take advantage of the same technology, data, and environment to mislead and disrupt through deception.

being deployed with increasing frequency at airports around the world. It will not be long before these same biometric capabilities and others are used for identity-verification purposes in banks and other businesses throughout metropolitan areas, as well as online. Vocord, a Russian company, has already developed a prototype covert facial recognition tool that can overcome shadows and other long-standing problems with facial data collection of the past: "Conceivably, the technology could be linked to police databases across Russia, notifying law enforcement as individuals of interest . . . are recognized."[19] The widespread use of these technologies poses a significant threat to both the clandestine military collector and the warfighter, as well as to the insurgent and the terrorist who benefit by hiding in plain sight—something that is more difficult in an operating environment that can find you. Alias travel becomes impossible, and operational meetings conducted in an assumed name may be uncovered before they occur.

Imagine being able to collect the biometric signature of an operative entering your city to meet with a clandestine source. As the head of the security service, you could run the data collected at the airport on every foreign traveler through the Ministry of Interior's computers to see whether any one of these individuals ever traveled to your country before under a different name. In combination with other technologies, such as web cameras, link analysis, and other predictive analytics, you would be able to not only identify the true names and affiliations of travelers but also track their movements and identify both the people they meet and those with whom they traveled or have had contact in the past. If you are one of these travelers, then it would be useful to know all of this ahead of time and plan accordingly. Not doing so would be dangerous and negligent.

Technological breakthroughs over the past several years have increased the speed by which biometric data are acquired over longer distances.

Attempts to spoof these systems are unlikely to work for either side because they contain built-in counterdetection capabilities, and because the traveler will not have up-to-date information about what biometric system is being used at a given location. Computer algorithms, for example, will be able to sense the "liveness" of the target.[20] The risk of wearing a fake iris or latex fingerprint is too high and would threaten immediate exposure. It would be safer and easier simply to travel in true name and have a reasonable story for being there. In addition, passive iris-collection capabilities and databases are expanding. India's Unique Identity Project to collect and store identifying information on its citizens, for example, will further enhance the efforts of its police and security services to track criminals and locate its citizens, at least in major urban areas.[21]

Technological breakthroughs over the past several years have increased the speed by which biometric data are acquired over longer distances and the speed by which the data can be retrieved and verified.[22] In the field of fingerprint collection, *contactless acquisition* is one of the fastest-growing research areas.[23] In the field of facial recognition, Facebook has one of the most widely used programs. As users upload their photos, Facebook provides immediate name suggestions to "tag" as friends. Some merchant outlets have begun using applications that allow customers to "pay by face,"[24] and

apartment complexes in New York City are beginning to migrate from keycards to keyless facial-recognition door sensors.[25] While mainstay biometric signatures, such as iris, fingerprint, and facial recognition, continue to be improved upon, advances in pulse and voice detection and other *soft biometric identifiers*, such as gait, gender, skin color, and height, will be added as metrics for collection. Add still further, the speed, rhythm, and general way a person types can be a way of determining identity and emotion.[26] The amalgamation of these signatures will only increase the accuracy and reliability of analysis.

Deception Detection

Stress Detection

Thermal imaging (which remotely reads the heat signature on your face; see Figure 1), voice-stress analysis (which measures the fluctuations in speech during periods of heightened stress), and other sensors are being used with increasing frequency at some foreign airports and by some foreign insurance companies to authenticate claims and detect fraud during face-to-face meetings and phone interviews with applicants and travelers.[27] Despite the healthy debate about the science behind these efforts at deception detection, practitioners in government and the commercial sector are moving ahead and are finding some of these technologies useful as ways to enhance the way all types of interviews are conducted. Immigration officers at one particular foreign airport in 2009, for example, openly monitored the voice stress of travelers who were waiting in line to enter the country.[28] They were able to uncover numerous fraudulent passports over a period of several months that would have gone unnoticed if they had been unable to identify candidates for secondary interviews. Closer scrutiny of their documents revealed photo substitutions and other irregularities. The immigration officers normally would not have the additional time needed for such close scrutiny.

Remote thermal imaging has also moved out of the lab and into public use as a resource-management tool. Some police departments now use this technology to interview suspects.[29] There is only so much time and only so many detectives available to pursue a given number of criminal leads. The faster they can filter out those who are confident in their stories, the faster they can focus attention on the most likely suspects. This technology could offer significant benefits in any similar secure interview setting (safe house or embassy walk-in room) where a military intelligence officer might need to validate the claims of an unproven clandestine

Figure 1. Thermal Imaging

SOURCE: Image by Hotflashhome, used in accordance with CC BY-SA 3.0.
RAND *PE181-1*

As more of daily life moves onto the Internet and into the realm of the virtual, verification and authentication will become mandatory, persistent, and commercially available to businesses, governments, and individual users.

source who is offering information about a threat to U.S. forces and facilities. The technology could be used further to indicate behavioral changes in a relationship with an otherwise vetted source and to provide early warning by prescreening terrorist informants who might pose a threat. In each of these cases, these technologies would supplement rather than supplant various other methods currently used to validate sources and their information. The technology also could be used to quickly prescreen local guard force applicants at U.S. embassies and military facilities—all of which are prime targets for al-Qa'ida and other jihadist groups.

In time, thermal imaging, voice-stress analysis, and other types of remote sensing technologies that are already being used in the medical industry to measure patients' vital signs are likely to be designed with algorithms to record person-specific data (such as thermal vasculature) as a means of identification. Thermal imaging and voice stress in particular are likely to be designed in form factors small and light enough for soldiers to carry and use during raids to protect themselves. For example, during a raid where only the family members of a terrorist or insurgent remain in the targeted house, the intelligence officer on the team could more quickly determine (as these technologies advance) which member of the family might be willing to talk and provide useful information, some of which might be time sensitive and contribute to force protection.

Syntax and Word Count Online

The trust and reliability required for the rising number of business and social relationships online has led to an increased interest in detecting deception in text. Deceivers use certain words and expressions as bridges in conversation to hide their intentions.[30] They do this in different ways from, and more frequently than, truth tellers. Being able to distinguish these patterns in an email message could enable people to tell whether the writer is trying to deceive the reader, whether it is one or two individuals doing the writing, and perhaps whether it is the same person writing each message.[31] This technology is commercially available and is on the threshold of becoming widespread. Being aware of how to use this type of technology to your advantage and how to guard against it being used against you is the first step. The second step is in determining whether the person writing the message is actually real or simply a bot that has been programmed to engage in conversation with you. The technology that permits you to determine whether or not the person writing the email is real has serious implications, once implemented, for attempts (official and criminal) to seed databases with alias personas and to hide in plain sight on the Internet. In short, as more of daily life moves onto the Internet and into the realm of the virtual, verification and authentication will become mandatory, persistent, and commercially available to businesses,

governments, and individual users. Terrorists and criminals will have the same access everyone else has. Their capabilities in this area will need to be factored into all online police, security, and intelligence operations.

Big Data Analytics

As deception-detection capabilities are refined and expand in use, they will be coupled with predictive analytical packages and an ever-increasing ability to burrow deeply into the public (and perhaps private) records of an individual's activities, online and off. Current link analysis and big-data analytic software already enable businesses to watch individuals' habits and to track, log, and map their locations, sentiments, social contacts, and behaviors automatically.[32] These tools, although limited when used alone, can be coupled with biometric sensors to further complete what is known as *life logging* and to provide "data-guided insight."[33] The digital exhaust left by just about everyone online through social media, commercial purchases, gaming, and other activities provides businesses, as well as governments and crime syndicates, with a wealth of data to mine and manipulate.[34] Staying offline might be safer but would itself be an anomaly or a sign that you are different and perhaps trying to hide something. A good counterintelligence service would key in on this type of signature and would try to find out more, which is precisely what an intelligence officer would not want. For example, someone posing in alias as a German banker to get closer to a particular intelligence target could be easily uncovered if his digital identity did not show that he has always been a German banker—i.e., he went to the right schools, belongs to the right social clubs, is connected to the right people, and looks more or less like every other person in his profession. All of this information is immediately findable—which makes hiding in plain sight difficult unless you are who you say you are. This has obvious, serious implications for how the military intelligence community recruits, trains, and deploys its officers. The ability to seed databases with any degree of reliability ahead of time with alias or synthetic personalities is unrealistic given the costs involved and scope of data available over time.

On the other side of the ledger, these capabilities can be combined with historical and cultural data to help project, if not predict, the movements of enemy forces. If throughout history enemy commanders from a particular nation have responded to A (e.g., a given military maneuver) by doing B, then it is at least statistically likely they will do so again. If every time a foreign leader has used a particular expression or metaphor in a speech, her country has undertaken an aggressive action against a neighboring nation, then it is possible the same thing will happen again. Using the data to unearth these patterns can help determine the likelihood of certain behaviors and create opportunities, both diplomatic and military, which in turn can help focus and otherwise refine intelligence collection. As a field of inquiry, big-data analytics has the power to

The digital exhaust left by just about everyone online . . . provides businesses, as well as governments and crime syndicates, with a wealth of data to mine and manipulate.

mine open-source literature and media to make foreign policy and warfare more predictive.[35]

Surveillance

Webcams

The growing presence of webcams throughout the downtown areas of cities around the world conjures up visions of Big Brother in George Orwell's novel *1984*. The presence of large numbers of cameras linked to the Internet and to security operations centers, however, is a reality today (see Figure 2). They are not everywhere in every city but are likely to be required as part of all urban landscapes in the future. For example, it is safe to say that there are tens of thousands of cameras in the "ring of steel" around downtown London and an even larger number deployed in downtown Beijing.[36] The Lower Manhattan Security Initiative in New York City ties an unspecified number of these webcams (perhaps as many as 2,000 cameras and 100 license plate readers, as well as other sensors) in the Wall Street area to a police operations center.[37] Eventually, webcams and sensors will cover the entire island and its ports of entry. This is a trend that will influence similar projects in other cities. The cameras and sensors alone are enough to make people look over their shoulders. When coupled with pattern-recognition software and advanced/predictive analytics, the potential disruptive impact that these networks of surveillance cameras will have on human behavior (criminal or otherwise) becomes undeniable.[38] Anyone intent on breaking a law in a city where these technologies are deployed will have to take into consideration the range and capabilities of these cameras and their accompanying technologies when planning an operation, even one as straightforward as casing a facility. If you do not usually belong in a given area, you could

Figure 2. London's Ring of Steel

SOURCE: Adapted from Carrick Mollenkamp and Christine Haughney, "'Ring of Steel' for New York?" *Wall Street Journal*, January 25, 2006.
RAND *PE181-2*

be recorded as an anomaly worth identifying and worth further tracking and investigation. In turn, intelligence officers could use the open webcams of a city and apply the same pattern-recognition software and analytics for countersurveillance and early warning to determine what a particular street in a particular area looks like on a normal day (since most people come and go the same way to the same places according to a daily routine) and what the street looks like on the day your intelligence operation will take place. These capabilities will continue to grow in access and availability and in the speed with which video can be searched and combined with other biometric technologies to quickly identify and track related individuals in a moving crowd.[39]

Car Telematics

The entertainment and diagnostic systems in modern cars enable manufacturers, rental car companies, police, and others to gain remote access to almost any vehicle. Information flows freely in and out of every new car and truck. Current trends show that vehicles are becoming automated to the point of eventually driving themselves. Within an urban environment, these same telematics could be used to locate and otherwise track every car in every neighborhood over time and distance. Yet again, with the application of pattern-recognition software and advanced analytics, this technology will enable businesses, security services, and perhaps crime syndicates to establish and recognize behavioral patterns, similar to the way the control of cell phone towers can be used to identify and track people. Cars that do not belong in certain locations would stand out and be scrutinized as suspicious and worth recording and inspecting. The ability to locate and track a vehicle, as well as monitor the passengers' conversations through wireless systems, will make police and counterintelligence work much easier and more predictive. The ability to remotely stop a car, lock the doors, and explode the airbags will make police and counterintelligence officers' jobs safer—eliminating the danger of shoot-outs during criminal arrests and counterterrorist renditions. In turn, each of these new capabilities will be highly disruptive to those on the receiving end.[40]

Telematics technology is heavily used today in commercial transportation and is expected to grow, particularly in Europe, from 1.5 million users in 2010 to an estimated 44 million by 2017. The largest market is likely to remain automotive: for fleet management and monitoring, GPS navigation, and predictive and early warning. However, few barriers exist to impede growth and integration into other sectors, such as social media platforms to provide real-time locational data on customers for product deliveries, faster wireless networking, and insurance.[41]

Drones

Cities and businesses worldwide already are exploring the use of small, unmanned aerial vehicles (UAVs) as a way to enhance police surveillance, traffic monitoring, and pizza delivery (see Figure 3). Regulatory issues aside, the most likely future is their widespread use. As they become quieter, they will be able to blend more read-

Figure 3. Civilian Quadracopter Drone

SOURCE: "Quadcopter Coaxial—OnyxStar FOX-C8 XT Observer from AltiGator," image by ZullyC3P, used in accordance with CC BY-SA 4.0.
RAND *PE181-3*

ily with the landscape and be harder to detect. They will be even more-formidable allies for law enforcement and security services when combined with other technologies, such as video, pattern-recognition software, data analytics, and any variety of sensors that will fit on the platform. Flown over selected roads in a war zone, such as the main streets of Kabul, Afghanistan, a drone equipped with this particular array of technologies could detect and track terrorists embedding an improvised explosive device alongside a road at night for remote detonation when a U.S. military convoy passes by in the morning. Other types of drones can already be used by military forces and intelligence collectors to determine the location of enemy movements to gain early warning and tactical advantage. In turn, however, terrorists can benefit by using drones to case an otherwise remote, heavily guarded facility to assess its vulnerabilities and to plan for an attack. Security officials need to take all of these potential uses into consideration when considering force protection and the susceptibility of embassies and government facilities to attack—something that has been underscored in recent years by the repeated violations of controlled airspace by drones in Washington, D.C. Electronic jamming in given areas might be one simple, low-cost way to defeat the threat.

Rapid advances in UAV technology development, application, and user innovation are expected to continue over the next five years and into the foreseeable future. Investments in research and development by Lockheed Martin, Boeing, Northrop Grumman, and AeroVironment, along with current military and commercial use, confirm the trend. Privacy concerns continue to mount, but the Federal Aviation Authority still expects that approximately 7,500 UAVs will be in the air by 2020. The Association for Unmanned Vehicle Systems International predicts that the drone industry will be worth $82 billion globally in 2025 and that civilian use will be fueled by advances in power, fuel consumption, communications, encryption, interoperability, and ease of use, as well as varying new levels of autonomy.[42]

Virtual Reality

The blending of real-world activities with the virtual has become more commonplace in cities over the past several years and is likely to continue to shape financial transactions, entertainment, and social and business relationships.[43] Augmented reality games and social networking virtual worlds, such as Second Life (see Figure 4) and Twinity, blur the distinctions between real and virtual by incorporating real-world technologies and activities, such as cell phone conversations, advertising, and marketing, as well as the sale of goods (both real and virtual) into a virtual space or game. Police

Figure 4. Second Life (Social Networking/Virtual Reality)

SOURCE: Image by HyacintheLuynes, used in accordance with CC BY-SA 3.0.
RAND *PE181-4*

departments, for example, have complained in recent years about how disruptive some of these augmented reality games can be when information from a virtual space is used to locate, track, and attack or kidnap other participants in the game on the streets of a real city.[44]

Business and intelligence relationships between avatars in a purely virtual space can be beneficial by helping compress the time and space needed to develop a relationship or to close a deal (such as recruiting new sources of information or simply meeting with them to collect information). This capability would be especially helpful when face-to-face meetings over lunch or dinner are not possible, because one person is in China and the other is in Europe, or because the military asset or source lives in a hostile or otherwise denied area or a war zone, where operations are excessively risky. Meeting with an avatar might also more appropriately fit the person's lifestyle, whereas a personal meeting might make him stand out, because it was something he would not normally do.

Being able to conduct these types of meetings for business or other purposes would first require considerable study and knowledge of what can be done securely. Everything resides on a server somewhere, but not everything is noticeable, especially if the activity fits the behavior of the participants in the game or in that particular virtual space, and not everything is stored forever. This particular combination of technologies in time and space, nevertheless, is creating a new sociology and is just one more example of an emerging trend that is dramatically changing how human beings interact and use a cityscape.[45]

Other Technology Trends to Watch

Combine all of the technologies noted above with an urban environment that is completely interconnected through a *wireless* mesh network. Add *cognitive computing*[46] and the arrival of advanced *robotics* (and drones)[47] armed with sensor platforms for both general surveillance and safety, as well as to facilitate the flow of traffic for people and cars in crowded areas. Add further the spread of *do-it-yourself 3-D manufacturing*,[48] which could enable some individuals to make their own weapons and step off the grid in some areas, along with *nanomaterials and synthetic biology*, which might eventually offer ways to counter biometric identification systems that are more reliable than those currently available and transform the way we communicate. These innovations and changes are likely to be gradual and absorbed as they are introduced into the fabric of an urban environment. How they will shape behavior and, in turn, be shaped or redirected by daily use is uncertain. However, there is little doubt that this is the direction in which our cities—the places where most people live, work, and play—are heading. Understanding more about how these technologies work and where and in

The U.S. defense intelligence enterprise will need to know much more about these disruptive combinations of technologies in order to navigate properly within the confines of a city or a war zone in the future.

what numbers they are deployed is essential for the warfighter and military intelligence collector alike.

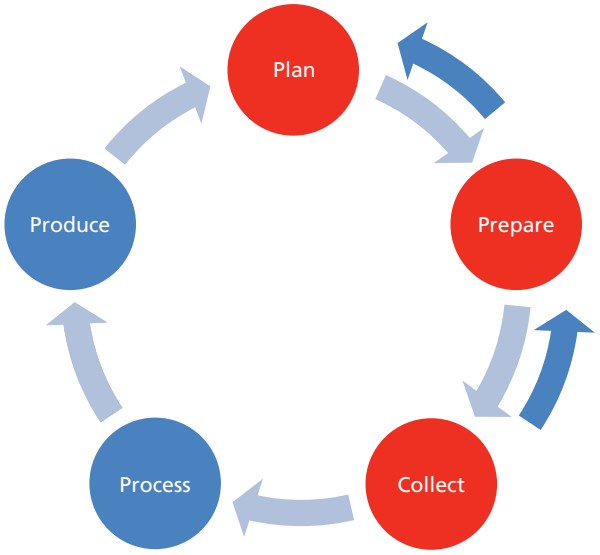
Assessment and Recommendations

The U.S. defense intelligence enterprise will need to know much more about these disruptive combinations of technologies in order to navigate properly within the confines of a city or a war zone in the future. Its officers will need and will want to know how these technologies work, where they are deployed, and what they mean for living and working, transportation, education, health, safety, and personal relationships. Gaining this type of awareness will require a focused effort to collect information and learn about things that officers have not had to pay attention to in the past. To avoid surprise, they will have to pay particular attention to the advantages and disadvantages of some of these inherently disruptive trends.[49]

Preparing for these changes and guarding against disruption and surprise, while at the same time taking advantage of what each new development in commercial technology offers, will require modifying the way clandestine operations are conducted currently. As illustrated in the intelligence collection and production cycle in Figure 5, the defense intelligence enterprise will need to focus more on collecting information about these potentially disruptive ideas, techniques, and technologies, and it will need to spend more time and money analyzing what they mean as both a counterintelligence threat to the way information is obtained and a means to enhance collection.

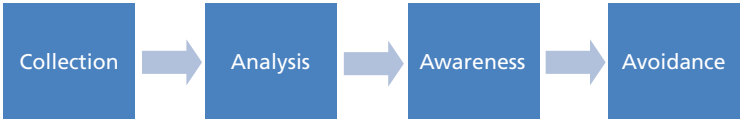
The following recommendations offer a road map (Figure 6) for making these changes.

Figure 5. Intelligence Collection and Production Cycle



RAND *PE181-5*

Figure 6. Road Map



RAND *PE181-6*

Collection

A new collection focus on commercial technologies will be necessary. It is not currently being done sufficiently or in an organized, systematic way that would support either military intelligence

A dedicated cadre of knowledgeable analysts will be needed to search for, review, and assess this new stream of collection for early warning of potential threats and for the benefits that could accrue from an awareness of how these new technologies could be used to enhance military intelligence operations and protect the warfighter.

operations or the warfighter, let alone other government personnel who travel, live, and work abroad. Some information about how commercial technologies are being used will have to be acquired by clandestine means. The vast majority of information on new commercial technologies, however, will be available from open sources and proprietary data held by businesses and departments of the government outside the intelligence community. Once located and acquired, the information could be centralized and compartmented in a database and made available to military intelligence analysts and operators, as well as others in the government who have a need to know the information's counterintelligence implications.

Analysis

A dedicated cadre of knowledgeable analysts will be needed to search for, review, and assess this new stream of collection for early warning of potential threats and for the benefits that could accrue from an awareness of how these new technologies could be used to enhance military intelligence operations and protect the warfighter. This effort will require hiring and training analysts who have technical backgrounds but who also understand military intelligence and the needs of the warfighter and the defense intelligence enterprise.

Awareness

Focused analytical and forensic assessments of the threats posed by these technologies will provide situational awareness of a given operating environment that can enable the intelligence collector and soldier to plan more effectively to either avoid the threat or otherwise counter it, if appropriate. Urban operating environments can be mapped to display the data on each of the technologies and to more fully present a digital display of the areas where it is hardest and, alternatively, safest to operate. This type of digital "thick mapping"[50] could include everything from the locations of web cameras and the ranges they cover to the locations of police stations, checkpoints, and enemy sympathizers. Knowledge about technologies that are harder to map, such as predictive analytics and virtual reality, can be made available on traveler and counterintelligence websites.

Avoidance

Avoiding the threat is likely to be the most reliable course of action. Current knowledge of the technologies arrayed within an urban environment against the collector, combined with an appreciation for how those technologies work and how they are used by foreign intelligence services and others, will provide a valuable baseline for planning but is unlikely to ever be current and detailed enough to

be reliable for operations. As a result, case officers would be unwise to rely on technical countermeasures. Jamming a GPS unit, for example, will always require greater knowledge of the physical surveillance threat. Likewise, the ability to effectively spoof a biometric system will require complete, up-to-the-minute knowledge of the system in place, how it works, and what upgrades have been made. Because of these knowledge requirements, few actual countermeasures are likely to be technical; all of them, however, will be critical to protecting the collector and the warfighter, who, unlike ever before, will need to know this type of counterintelligence information for the detailed operational planning they will need to do long before leaving home.

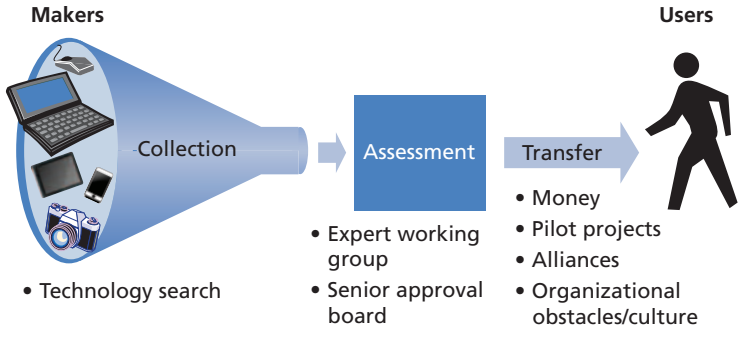
Strategic Technology Search

Being aware of technologies on the market and how they can be combined with other products and used in new ways will require a mechanism or series of processes that can systematically search for new technologies and that, in turn, can help analysts forecast trends in technology areas that are most likely to impinge on analysts' business areas. Intelligence Advanced Research Projects Activity's (IARPA's) Foresight and Understanding from Scientific Exposition (FUSE) program[51] is an example of how an analysis of new patents, scientific articles, and investments can be brought together to gain insight and to forecast where existing commercial technologies, such as facial recognition, are heading.[52] Other techniques for searching the market could tap into In-Q-Tel's strategic investment capabilities in this area and could use outside firms who specialize in particular technologies, such as communications or new materials.[53] In certain cases, some of this knowledge might already reside within the defense intelligence enterprise or the U.S. government at large.

Rapid Technology Transition

Designing a process by which to quickly bring new commercially available technologies into the workplace will help avoid the valley of death so often seen in the private sector, where new inventions never make it to market despite the need for them and the promise they hold. Innovation and change are always difficult. A process to aid senior managers in the decisionmaking required to bring new products and technology into the defense intelligence enterprise will help. One way to do this is described in Figure 7, which shows how to combine the processes discussed above to search for new technologies, assess them, and then present them to a board of senior decisionmakers (who know their business areas, such as HUMINT [human intelligence], SIGINT [signals intelligence], and logistics), with the aim of quickly getting the new capability into the hands of the soldier or case officer who needs it. There

Figure 7. Technology Transition Process



RAND *PE181-7*

A robust, multidisciplinary, and routine dialogue between users and makers is one of the best ways to ensure that users' needs are understood clearly and that products are designed properly and delivered as quickly as possible.

will continue to be a requirement for longer-term research and development, as well as for fundamental science, but an increasingly large number of defense intelligence needs can be addressed directly by commercial products requiring little or no modification. This process would supplement the military's existing acquisition efforts and current logistics focus on Silicon Valley and on leveraging commercial technologies through the Pentagon's Better Buying Power 3.0 program.[54]

In-Q-Tel is yet another resource that can be used to innovate and solve some of the defense intelligence enterprise's hardest problems by making strategic investments in new commercial technologies that offer solutions to pressing, immediate military needs—particularly in instances when these needs do not call for enough commercial production to entice or warrant investment by venture capital firms. This type of immediate, strategic investment can be vital when certain components are required for integration into larger, short-term development projects. Lighter-weight armor for protective clothing and vehicles used in war zones is one example of where this resource can come into play as a strategic search and assessment tool.

Engagement Between Users and Makers

A robust, multidisciplinary, and routine dialogue between users and makers is one of the best ways to ensure that users' needs are understood clearly and that products are designed properly and delivered as quickly as possible. Too often the absence of this type of dialogue leads to money being spent to produce what is thought to be needed but is not ultimately used. People will generally pay lip service to the need for collaboration and dialogue, but they rarely actually do it. Because of this organizational tendency to avoid coordinating and collaborating with others, a formal mechanism is needed to make that happen. The mechanism can be as simple as a regular working-group meeting to gauge progress on a given project and to exchange knowledge. Another method is to embed referents in the offices that share a mission. Yet another way is to collapse units working on the same mission under one roof as parts of a center or larger task force. In each case, the aim is to create a shared vision and sense of mission among people who too often regard "the other" as unimportant or outside the scope of their work. Organizational arrangements that help dissolve these barriers and create proximity between users and makers, as well as between employees and managers, will enhance production, innovation, and performance.

Conclusion

In the end, these commercial technologies are primarily about identifying and tracking people and patterns of behavior. Their presence is greatest in urban environments, which happen to be where

most military intelligence operations are conducted and where most future insurgencies and wars are likely to be fought. The combination of the technical and behavioral is the key to understanding these technologies, as is an experience-based approach to analyzing the scenarios in which each technology can be applied in unique ways, either alone or in tandem with others, as it becomes widely used in a given place and at a given time. Just because something can be done, however, does not mean that it will be done in every country or every city in the same way. The challenge is to understand what is possible in each place or each operating environment in advance and to be ready for it—i.e., to see how certain commercial technologies could be used to benefit military intelligence collection and warfighting and to avoid applications that could disrupt or otherwise harm those endeavors.

These commercial technologies are primarily about identifying and tracking people and patterns of behavior. Their presence is greatest in urban environments, which happen to be where most military intelligence operations are conducted and where most future insurgencies and wars are likely to be fought.

Notes

[1] The United States Census Bureau defines *urban areas* as those that are represented by densely developed territory that encompasses residential, commercial, and other nonresidential land use by 50,000 or more people. Urban clusters have at least 2,500 people but fewer than 50,000. See U.S. Census Bureau, "Urban and Rural Classification," web page, undated, www.census.gov/geo/reference/urban-rural.html (accessed April 6, 2016).

[2] See Adam Greenfield, *Everyware: The Dawning Age of Ubiquitous Computing*, Berkeley, Calif.: New Riders, 2006; Mark Shepard, *Sentient City: Ubiquitous Computing, Architecture, and the Future of Urban Space*, Cambridge, Mass.: MIT Press, 2011; and Peter Morville, *Ambient Findability*, Sebastopol, Calif.: O'Reilly Media, Inc., 2005. Also see Timothy Williams, "Police Cam Downside: Your Arrest Hits YouTube," *New York Times*, April 27, 2015, p. 13; James Canton, *Future Smart: Managing the Game-Changing Trends That Will Transform Your World*, Boston: De Capo Press, 2015.

[3] For a full discussion of this concept, see Eric von Hippel, *Democratizing Innovation*, Cambridge, Mass.: MIT Press, 2006. For a video that shows the widespread use of various surveillance and biometric technologies in New York City, see *Scientific American*, "New York City's Hidden Surveillance Network Part 2—by Scientific American," YouTube video, September 16, 2011, https://www.youtube.com/watch?v=LSf4YCB3Hi0&nohtml5=False (accessed April 20, 2016).

[4] The trend worldwide is toward increasing urbanization. Although there are exceptions, much military intelligence collection is and will continue to be conducted in urban environments, which is where many wars and insurgencies are fought and where most terrorist operations are carried out. For a good discussion of the future of insurgencies, see David Kilcullen's *Out of the Mountains: The Coming Age of the Urban Guerrilla*, New York: Oxford University Press, 2013.

[5] This assessment focuses exclusively on the general and innovative use of commercially available technologies and their potential impact on military HUMINT (human intelligence) operations and, by extension, the warfighter. Some of the concepts used in this report also could be applied to other forms of intelligence collection, such as SIGINT (signals intelligence). This assessment is not about research and development (R&D) in the Defense Intelligence Enterprise or in the larger intelligence community but does offer a way to augment the notion of *enhanced integrated intelligence* (the automated collection, analysis, integration, and discovery of relevant intelligence data from classified and open sources) put forth in the R&D policy and recommendations for the intelligence community in the 2013 National Commission for the Review of the Research and Development Programs of the United States Intelligence Community, *Report of the National Commission for the Review of the Research and Development Programs of the United States Intelligence Community*, Washington, D.C., 2013.

[6] There is a lively debate within the military and defense communities about the differences between *military* and *defense intelligence*. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, Washington, D.C.: Joint Chiefs of Staff, November 8, 2010 (amended October 15, 2015); and Joint Publication 2-0, *Joint Intelligence*, Washington, D.C.: Joint Chiefs of Staff, October 22, 2013, do not make the distinction but are useful reference documents on the general subject. For purposes of simplicity, in this report, *military intelligence* and *defense intelligence* are used interchangeably and refer to all manner of HUMINT intelligence-collection operations to discern the military, political, economic, technological, and other related capabilities and intentions of foreign enemies.

[7] Technologies that are combined and used in unique, new ways can be disruptive to both markets and armies. See Terry Pierce, *Warfighting and Disruptive Technologies: Disguising Innovation*, London: Frank Cass, 2004; David Johnson, *Fast Tanks and Heavy Bombers: Innovation in the U.S. Army*, Ithaca, N.Y.: Cornell University Press, 1998; Wilson W. S. Wong, *Emerging Military Technologies: A Guide to the Issues*, Santa Barbara, Calif.: Praeger Press, 2013; Stephen Peter Rosen, *Winning the Next War: Innovation and the Modern Military*, Ithaca, N.Y.: Cornell University Press, 1991; Michael O'Hanlon, *Technological Change and the Future of Warfare*, Washington, D.C.: The Brookings Institution, 2000; P. W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century*, New York: Penguin Press, 2009; and Richard W. Rubright, *The Role and Limitations of Technology in U.S. Counterinsurgency Warfare*, Lincoln: University of Nebraska Press, 2015. Also see Cathy N. Davidson, *Now You See It: How Technology and Brain Science Will Transform Schools and Business for the 21st Century*, London: Penguin Books, 2011; and Iqbal Qadir, "Form, Transform, Platform: How the Ubiquity of Mobile Phones Is Unleashing an Entrepreneurial Revolution," *Innovations*, Vol. 7, No. 4, 2012, pp. 3–12.

[8] Craig Timberg, "Cellphones Used as Secret Trackers," *Washington Post*, August 25, 2014, pp. 1, 5.

[9] Curtis Wallen, "How to Make a Secret Phone Call," *Fast Company*, April 6, 2015, http://www.fastcompany.com/3044637/secret-phone-network (accessed April 7, 2016). This article was adapted from Wallen's handbook *Proposition for an On-Demand Clandestine Communication Network*, curtiswallen.com, 2015, http://curtiswallen.com/p2cn/ (accessed April 7, 2016).

[10] Peter Van der Windt and Macartan Humphreys, "Crowdseeding in Eastern Congo: Using Cell Phones to Collect Conflict Events Data in Real Time," *Journal of Conflict Resolution*, November 4, 2014, pp. 1–34.

[11] Adam Greenfield, *Everyware: The Dawning Age of Ubiquitous Computing*, Berkeley, Calif.: New Riders: 2006; Mark Shepard, *Sentient City: Ubiquitous Computing, Architecture, and the Future of Urban Space*, Cambridge, Mass.: MIT Press, 2011; Julia Angwin, *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*, New York: Henry Holt, 2014; Peter Morvilla, *Ambient Findability*, Sebastopol, Calif.: O'Reilly Publishers, 2005; Anthony Townsend, *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia*, New York: W.W. Norton and Co., 2013; Marc Goodman, *Future Crimes: Everything Is Connected, Everyone Is Vulnerable, and What We Can Do About It*, New York: Doubleday, 2015.

[12] Abby Ohlheiser, "The Controversial GPS Device That Helped Police Catch Carlesha Freeland-Gaither's Alleged Abductor," *Washington Post*, November 7, 2014.

[13] For a good overview of the technology, see Sanjay Sarma, "How Inexpensive RFID Is Revolutionizing the Supply Chain," *Innovations*, Vol. 7, No. 3, 2012, pp. 35–52.

[14] Walter L. Perry, Brian McInnis, Carter C. Price, Susan Smith, and John S. Hollywood, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, Santa Monica, Calif.: RAND Corporation, RR-233-NIJ, 2013, http://www.rand.org/pubs/research_reports/RR233.html (accessed April 11, 2016); Priscillia Hunt, Jessica Saunders, and John S. Hollywood. *Evaluation of the Shreveport Predictive Policing Experiment*, RAND Corporation, RR-531-NIJ, 2014, http://www.rand.org/pubs/research_reports/RR531.html (accessed April 11, 2016); Keith Gierlack, Shara Williams, Tom LaTourrette, James M. Anderson, Lauren A. Mayer, and Johanna Zmud, *License Plate Readers for Law Enforcement: Opportunities and Obstacles*, RAND Corporation, RR-467-NIJ, 2014, http://www.rand.org/pubs/research_reports/RR467.html (accessed April 11, 2016).

[15] An early look at this set of problems is Lt. Col. H. R. McMaster, *Crack in the Foundation: Defense Transformation and the Underlying Assumption of Dominant Knowledge in Future War*, Carlisle, Pa.: Center for Strategic Leadership at the U.S. Army War College, Student Issue Paper, Volume S03-03, November 2003.

[16] Wireless mesh networks are communications networks made up of nodes organized in a mesh of devices, such as laptops and cellphones, that uses routers to forward the traffic to and from gateways that may or may not be connected to the Internet.

[17] H. James Wilson, "Wearables in the Workplace," *Harvard Business Review*, September 2013, p. 23. For further reading on the varied topic of ambient sensing, see Cesar Benavente-Peces, Andreas Ahrens, and Joaquim Filipe, "Advances in Technologies and Techniques for Ambient Intelligence," *The Journal of Ambient Intelligence and Human Computing*, Vol. 5, 2014, pp. 621–622; Tetsushi Ikeda, Hiroshi Ishiguro, Takahiro Miyashita, and Norihiro Hagita, "Pedestrian Identification by Associating Wearable and Environmental Sensors Based on Phase Dependent Correlation of Human Walking," *The Journal of Ambient Intelligence and Human Computing*, Vol. 5, No. 5, 2014, pp. 645–654; Paul Marks, "Seek and Ye Shall Find," *New Scientist*, August 10, 2013, p. 19; Clive Thompson, "Good Vibrations: Tech That Talks Through Your Skin," *Wired*, January 2015, p. 26; Kim Tingley, "The Body Electric: A Scientist Takes Computing Power Under the Skin," *The New Yorker*, November 25, 2013, pp. 78–86; Ariana Eunjung Cha, "The Revolution Will Be Digitized," *Washington Post*, May 10, 2015, pp. 1, 10.

[18] Jason Thomson, "Bendable Wallpaper Cameras Are Right Around the Corner," *Christian Science Monitor*, April 16, 2016, http://www.csmonitor.com/Technology/2016/0416/Bendable-wallpaper-cameras-are-right-around-the-corner (accessed May 9, 2016).

[19] Trevor Aaronson, "Face Value: Could Recognition Software Be the Next Frontier in Russian Snooping?" *Foreign Policy Magazine,* May/June 2015, p. 58.

[20] Kasper Rasmussen, Marc Roeschlin, Ivan Martinovic, and Gene Tsudik, "Authentication: Using Pulse-Response Biometrics," paper presented at the Network and Distributed Systems Security Symposium, San Diego, Calif., February 2014.

[21] Hoe Pei Shan, "ICA Looking into Iris Scanning," *Asia One Travel News*, September 28, 2014.

[22] "Gatwick Unveils Iris at a Distance Biometric Security," *Information Age*, October 19, 2011.

[23] National Law Enforcement and Corrections Technology Center, "Evaluating the Next Generation of Fingerprint Technology," *TECHBeat*, Fall 2013, p. 11.

[24] Tim De Chant, "The Boring and Exciting World of Biometrics," *NOVA Next*, PBS, June 18, 2013, http://www.pbs.org/wgbh/nova/next/tech/biometrics-and-the-future-of-identification (accessed April 11, 2016).

[25] Doug Bonderud, "Biometric Security: Intelligent Home Defense?" *Digital Landing*, March 12, 2014, http://www.digitallanding.com/biometric-security-home-defense/ (accessed April 7, 2016).

[26] Aviva Rutkin, "Emailing Angry: Your Keyboard Feels Your Pain," *New Scientist*, August 30, 2014, p. 20.

[27] "Lie Detectors 'Cut Car Claims,'" *BBC News*, October 30, 2003, http://news.bbc.co.uk/2/hi/uk_news/3227849.stm (accessed April 7, 2016); "How Do Telephone Lie Detectors Work?" *BBC News*, September 7, 2007, http://news.bbc.co.uk/2/hi/uk_news/magazine/6983359.stm (accessed April 7, 2016); Hal Hodson, "Hang on Your Every Word: Voice-Analyzing Tool Helps People Judge Your Emotions," *New Scientist*, May 10, 2014, p. 20; Hamish Pritchard, "New Emotion Detector Can See When We're Lying," *BBC News*, September 13, 2011, http://www.bbc.com/news/science-environment-14900800 (accessed April 7, 2016); Rachel Metz, "Voice Recognition for the Internet of Things," *MIT Technology Review*, Vol. 118, No. 1, 2014, p. 21.

[28] This information is drawn from the author's personal interview with these immigration officials at the time. See Nemesysco, "Nemesysco's Layered Voice Analysis (LVA™)," Nemesysco.com, undated, http://nemesysco.com/speech-analysis-technology (accessed April 12, 1016); also see Nemesysco, "LVA 6.50 Investigation Focus Tool," Nemesysco.com, undated, http://nemesysco.com/security-investigation-lva650 (accessed April 20, 2016); J. Michael Adler, "Detecting Deceptive Responses in Sex Offenders: A Comparison of Layered Voice Analysis and the Polygraph," unpublished manuscript, 2009; William Mayew and Mohan Venkatachalam, "The Power of Voice: Managerial Affective States and Future Firm Performance," unpublished manuscript, Duke University Fuqua School of Business, January 20, 2011.

[29] This information is drawn from the author's personal interview with U.S. police officials in 2009. Also see "Secret Weapon: How Thermal Imaging Helped Catch Bomb Suspect," *NBC News*, April 19, 2013, http://usnews.nbcnews.com/_news/2013/04/19/17830076-secret-weapon-how-thermal-imaging-helped-catch-bomb-suspect?lite (accessed April 7, 2016). For more on the commercial availability of thermal imaging as an iPhone application, see "Thermal Imaging Gets More Common but the Courts Haven't Caught Up," *All Tech Considered*, NPR, February 27, 2015.

[30] Peter Aldhous, "Language of Deceit Betrays Scientific Fraud," *New Scientist*, September 6, 2014, p. 14; Hal Hodson, "Nothing but the Truth: Google Is Looking at Ways to Reward the Most Trustworthy Websites," *New Scientist*, February 28, 2015, p. 24.

[31] For a detailed explanation of linguistic inquiry and Word Count, see Jeffrey Hancock, "Lies in Conversation: An Examination of Deception Using Automated Linguistic Analysis," *Proceedings of the 26th Annual Conference of the Cognitive Science Society*, Mahwah, N.J.: Lawrence Erlbaum Associates, 2005; Yla R. Tausczik and James W. Pennebaker, "The Psychological Meaning of Words: LIWC and Computerized Text Analysis Methods," *Journal of Language and Social Psychology*, Vol. 29, No. 1, 2010, pp. 24–54; and Judee Burgoon, J. P. Blair, Tiantian Qin, and Jay F. Nunamaker, Jr, *Detecting Deception Through Linguistic Analysis*, Heidelberg: Springer-Verlag, 2003; Aldert Vrij, Pär Anders Granhag, and Stephen Porter, "Pitfalls and Opportunities in Nonverbal and Verbal Lie Detection," *Psychological Science in the Public Interest*, Vol. 11, No. 3, 2010, pp. 89–121; James W. Pennebaker, *The Secret Life of Pronouns: What Our Words Say About Us*, New York: Bloomsbury Press, 2011; and Paul Marks, "Lie All You Like, I Can Still Identify You," *New Scientist*, May 19, 2007.

[32] Albert-Laszlo Barabasi, *Linked: How Everything Is Connected to Everything Else and What It Means for Business, Science, and Everyday Life*, New York: Basic Books, 2014; Nathan Eagle and Kate Greene, *Reality Mining: Using Big Data to Engineer a Better World*, Cambridge, Mass.: MIT Press, 2014; Eric Siegel, "Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie or Die," Hoboken, N.J.: John Wiley and Sons, 2013; Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, New York: Houghton, Mifflin, Harcourt, 2013; "Move Over, Siri: Predictive Intelligence; A New Breed of Personal-Assistant Software Tries to Anticipate What Smartphone Users Want, Before They Ask for It," *The Economist*, November 30, 2013; Alex Pentland, *Social Physics: How Good Ideas Spread—The Lessons from a New Science*, New York: Penguin Press, 2014; Evgeny Morozov, "Every Little Byte Counts: The Ubiquity of Data Gathering Has Staggering Implications for Understanding, Predicting, and Influencing Human Behavior," *New York Times Book Review*, May 18, 2014; Aviva Rutkin, "Credit Card Bills Make You Easy to Identify," *New Scientist*, February 7, 2015, p. 21.

[33] Steve Lohr, "Unblinking Eyes Track Employees," *New York Times*, June 22, 2014, p. 15.

[34] Mark Guarino, "Can Math Stop Murder? In a Besieged Chicago, Big Data May Help Curb Gang Violence," *The Christian Science Monitor*, July 21, 2014, p. 27; Andrew Marantz, "The Virologist: How a Young Entrepreneur Built an Empire by Repackaging Memes," *The New Yorker*, January 5, 2015, p. 20; Douglas Heaven, "Trouble on the Horizon: A Database of World Events Could Help Predict How Conflicts Will Play Out," *New Scientist*, May 11, 2013.

[35] For more on the predictive potential of big-data analytics, see Cale Guthrie Weissman, "Inside the Company that Can Predict the Future by Analyzing Every Piece of Information on the Web," *Business Insider*, May 26, 2015.

[36] "BBA and Police Work to Create 'Virtual Ring of Steel' Around City of London," British Bankers' Association, February 10, 2103, https://www.bba.org.uk/news/press-releases/8850-2/ (accessed April 11, 2016); Sylvia Hui, "Bloomberg Reviews London's Ring of Steel," Associated Press, May 11, 2010.

[37] Larry Greenemeier, "The Apple of Its Eye: Security and Surveillance Pervades Post-9/11 New York City," *Scientific American*, September 9, 2011.

[38] For a current account of how webcams are being used for surveillance, see Paul Marks, "Windows on the World: A Software Flaw Means It's Easy to Peek at What Everyone Else Is Up To," *New Scientist*, February 9, 2013, p. 24; Shane Harris, "The Social Laboratory: Singapore Is Testing Whether Mass Surveillance and Big Data Can Not Only Protect National Security, but Actually Engineer a More Harmonious Society," *Foreign Policy Magazine*, July/August 2014, p. 64; Timothy Williams, "Police Cam Downside: Your Arrest Hits YouTube," *New York Times*, April 27, 2015, pp. 1, 13.

[39] Jim Nash, "The Tiny Spy: A Matchstick-Sized Sensor Can Secretly Locate and Record a Conversation in a Busy Public Space," *New Scientist*, September 28, 2013, p. 21; Rachel Nuwer, "Kinect Cameras Look for Kicks and Punches," *New Scientist*, November 9, 2013, p. 22; Steve Lohr, "Unblinking Eyes Track Employees," *New York Times*, June 22, 2014, p. 15; Aviva Rutkin, "Off the Clock, On the Record: More and More Firms Are Digitally Tracking Their Employees—At Work, Rest, and Play," *New Scientist*, October 18, 2014, p. 22; Aviva Rutkin, "Police in the Spotlight: Body Cams and Apps May Keep the Police in Check," *New Scientist*, August 30, 2014, p. 22.

[40] For more on car telematics, see Damien Stolarz, *Car PC Hacks*, San Francisco: O'Reilly Media, 2005; Jamie Carter, "Telematics: What You Need to Know," *TechRadar*, June 27, 2012; James M. Anderson, Nidhi Kalra, Karlyn D. Stanley, Paul Sorensen, Constantine Samaras, and Oluwatobi A. Oluwatola, *Autonomous Vehicle Technology: A Guide for Policymakers*, Santa Monica, Calif.: RAND Corporation, RR-443-2-RC, 2016, pp. 57–63, http://www.rand.org/pubs/research_reports/RR443-2.html (accessed April 11, 2016).

[41] "2014 Countdown: 5 Telematic Trends to Watch For," Actsoft, December 30, 2013; "The Quest for Telematics 4.0," Ernst and Young, 2013; Egil Juliussen, "The Future of Automotive Telematics," *Business Briefing: Global Automotive Manufacturing and Technology*, 2003.

[42] James Winnefeld and Frank Kendall, *Unmanned Systems Integrated Roadmap FY2011–2036*, Washington, D.C.: U.S. Department of Defense, 2011; Shirley Li, "Biodegradable Drones," *The Atlantic*, November 17, 2014; Henry Holden, "Drones Fly into the Mainstream," *World Airnews*, Vol. 42, No. 1, 2014, p. 38; Matt Egan, "6 Companies Behind the Drone Revolution," *CNN*, August 6, 2014.

[43] For further details, refer to Edward Castronova, *Exodus to the Virtual World: How Online Fun Is Changing Reality*, New York: Palgrave, 2007; Hal Hodson, "Tech to the Streets: Google's New Augmented Reality Game Sees Players Wage a Turf War in Their Own City—But What's It Really About?" *New Scientist*, December 1, 2012, p. 19; Chris Baraniuk, "No Drone Zone: Technology to Ground Drones Is Taking Off," *New Scientist*, May 2, 2015, p. 22; "Copping a Copter: Dealing with Rogue Drones," *The Economist*, May 2, 2015, p. 69.

[44] *Augmented Reality Games*, video, Washington, D.C.: The Open Source Center, 2007.

[45] For more information on this trend, see James Canton, *Future Smart: Managing the Game-Changing Trends That Will Transform Your World*, Boston: Da Capo Press, 2015, pp. 115, 144, 150, 201; Martin Van Creveld, *Wargames: From Gladiators to Gigabytes*, Cambridge, UK: Cambridge University Press, 2013; Michael Clune, *Gamelife: A Memoir*, New York: Farrar, Straus and Giroux, 2015; John C. Beck and Mitchell Wade, *The Kids Are Alright: How the Gamer Generation Is Changing the Workplace*, Boston: Harvard Business School Press, 2006; Thomas Malaby, *Making Virtual Worlds: Linden Lab and Second Life*, Ithaca, N.Y.: Cornell University Press, 2009; and Wagner James Au, *The Making of Second Life: Notes from the New World*, New York: Harper-Collins, 2008.

[46] For more on the new machine age, see Erik Brynjolfsson and Andrew McAfee, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Machines*, New York: W. W. Norton & Company, 2014.

[47] For a current review of drones already in use, see Lev Grossman, "Rise of the Drones," *Time*, February 11, 2013, pp. 29–33. For a good review of current developments in automation, see Nicholas Carr, *The Glass Cage: Automation and Us*, New York: W. W. Norton, 2014.

[48] For a current survey of additive manufacturing, see Chris Anderson, *Makers: The New Industrial Revolution*, New York: Crown Business, 2012. Also see Jeroen P. J. De Jong and Erik De Bruijn, "Innovation Lessons from 3-D Printing," *MIT Sloan Management Review*, Winter 2013, p. 43; Henry Fountain, "Tools of Modern Gunmaking: Plastic and a 3-D Printer," *New York Times*, January 29, 2013; Dane Strangler and Kate Maxwell, "DIY Producer Society," *Innovations*, Vol. 7, No. 3, 2012, pp. 3–10; Andy Greenberg, "AR-15 Secret Weapon," *Wired Magazine*, June 3, 2015, pp. 76–83.

[49] Terry Pierce in *Warfighting and Disruptive Technologies: Disguising Innovation* (London: Frank Cass, 2004) illustrates this concept by looking at the development and use of the tank in combat. The tank was developed by the British in World War I but was not used effectively or innovatively until German General Heinz Guiderian combined it with infantry, radios, and airplanes. His "blitzkrieg" was a complete surprise to the French, even though the trends could be seen and the technologies were already known. Blitzkrieg was a disruptive innovation.

[50] For more on the concept of *thick mapping*, see Todd Presner, David Shepard, and Yoh Kawano, *Hyper Cities: Thick Mapping in the Digital Humanities*, Cambridge, Mass.: Harvard University Press, 2014. For more on technology forecasting and foresight, see Luke Georghiou, et al., *The Handbook of Technology Foresight: Concepts and Practice*, Cheltenham, UK: Edward Elgar, 2008.

[51] Intelligence Advanced Research Projects Activity, "Foresight and Understanding from Scientific Exposition (FUSE)," undated, http://www.iarpa.gov/index.php/research-programs/fuse (accessed April 7, 2016); Tugrul Daim, Guillermo Rueda, Hilary Martin, and Pisek Gerdsri, "Forecasting Emerging Technologies: Use of Bibliometrics and Patent Analysis," *Technological Forecasting and Social Change*, Vol. 73, No. 8, 2006, pp. 981–1012.

[52] For more on patent analysis, see Christopher A. Eusebi and Richard Silberglitt, *Identification and Analysis of Technology Emergence Using Patent Classification*, Santa Monica, Calif.: RAND Corporation, RR-629-OSD, 2014, http://www.rand.org/pubs/research_reports/RR629.html (accessed April 7, 2016); Lu Huang, Yi Zhang, Ying Guo, Donghua Zhu, and Alan L. Porter, "Four Dimensional Science and Technology Planning: A New Approach Based on Bibliometrics and Technology Roadmapping," *Technological Forecasting and Social Change*, Vol. 81, 2014, pp. 39–48; Francis Narin, "Patent Bibliometrics," *Scientometrics*, Vol. 30, No. 1, 1994, pp. 147–155.

[53] In-Q-Tel identifies, adapts, and delivers innovative technical solutions to support its missions of the U.S. intelligence community (see its website, www.iqt.org).

[54] Patrick Tucker, "Pentagon Sets Up a Silicon Valley Outpost," *Defense One*, April 23, 2015; Amrita Jayakumar, "Pentagon Tunes Buying Strategy to Sharpen Technology Edge," *Washington Post*, April 10, 2015, p. 16; Daniel Goure, "The Pentagon Is Focusing on the Wrong Aspect of Commercial Innovation," Lexington Institute, May 29, 2015; Daniel Goure, "How the Pentagon's Acquisition System Dis-Incentivizes Business, Lexington Institute, May 11, 2015; Loren Thompson, "Five Reasons Why Silicon Valley Won't Partner with the Pentagon," *Forbes*, April 27, 2015.

About This Perspective

Commonplace commercial technologies can be combined and used in unique ways to reshape an urban environment and disrupt how we live and work, in the United States and abroad. The technologies are not new but are becoming ubiquitous and are being used in new ways. The technologies highlight a democratizing trend that gives more people the freedom and power to use any number of new, commercially available technologies to innovate and to challenge existing government rules and community practices. This democratizing trend, however, comes at a cost to privacy, security, and secrecy and is changing the way people interact socially and politically. It is changing the way we conduct business, diplomacy, intelligence operations, and war, the future of which is likely to be increasingly urban in nature.

This research was conducted within the Intelligence Policy Center of the RAND National Defense Research Institute, a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community.

For more information on the RAND Intelligence Policy Center, see www.rand.org/nsrd/ndri/centers/intel or contact the director (contact information is provided on the web page).

About the Authors

William Young is a senior policy analyst at the RAND Corporation. Young managed and led intelligence collection operations for the National Clandestine Service for over 30 years before he retired in December 2011. He served as the director of the Operations Technology Office and as the national intelligence manager for Yemen but spent most of his career in the Middle East and South Asia working on counterterrorism, counterinsurgency, and counterproliferation issues.

David Stebbins is a project associate at the RAND Corporation currently working on intelligence, emerging technology trends, and security cooperation. Prior to joining RAND, he worked for the New York Police Department's Counterterrorism Bureau and also worked as a national security legislative staff assistant for the Senate Judiciary Committee. Stebbins previously served in the Vermont National Guard as a combat infantry medic.

For more information on this publication, visit www.rand.org/t/PE181.

www.rand.org

PE-181-OSD (2016)