Contesting Key Terrain: Urban Conflict in Smart Cities of the Future

Maxim Kovalsky
Lieutenant Colonel Robert J. Ross, Ph.D.
Greg Lindsay

ABSTRACT

Smart City initiatives are multiplying at an accelerated pace. Hundreds of Smart City pilot projects are aiming to make urban dwelling more sustainable by leveraging automation, and digitizing interactions among technologies, people, and the physical environment. Each project is an ecosystem, with stakeholders ranging from government officials and technology firms with their near infinite supply chains to city residents. Many projects that began as experimental pilots are now integral to the way city government organizations deliver services to their constituents. An increasingly urbanized world, rapidly becoming more dependent upon sophisticated technologies, presents novel and substantial complexities to future military operations.

Smart Cities will become the status quo operating environment for future urban military operations. This article illustrates the implications of misestimating the impact of connected infrastructure during post-conflict operations in the networked urban environment of tomorrow and proposes a methodology to assess and manage risks associated with operating in densely networked environments. The authors rely on a combination of qualitative methodologies (Threatcasting, Thematic Analysis) to identify key technological trends being adopted by municipal governments around the world and to explore the implications these technologies pose for future military operations in urban environments. Based on their findings, the article presents eight supplemental questions to help military planners understand and anticipate vulnerabilities and opportunities associated with operating in Smart Cities, and otherwise improve operational decision-making and the prognosis for success in the urban battlespace.

Maxim Kovalsky is a Senior Manager in Deloitte's Cyber Risk Advisory practice. With over ten years of experience in technology and cyber security, Maxim's work at Deloitte has focused on security intelligence and operations strategy and implementation projects across multiple sectors. He has led engagements in areas covering cyber security program assessments, threat detection and response, and threat intelligence. Prior to joining Deloitte, Maxim worked for the Federal Bureau of Investigation, providing operational and intelligence support to complex cybercrime investigations. Mr. Kovalsky is a reservist in the U.S. Army and a member of the Cyber Electromagnetic Activities portfolio team within the 75th Innovation Command.

PREFACE

"They've turned the city against us," thought Major General Adam Larsen as he surveyed the smoking wreckage of several personnel carriers in the town square. The enemy was still nowhere to be seen, but it clearly was doing everything short of showing itself to expel his division out of the city. First, trash mountains began appearing atop overflowing waste bins at every intersection, attracting vermin. Then traffic signals malfunctioned, leading to citywide crashes and collisions. Then, most major thoroughfares became impassable as frustrated police cleared intersections while fending off rats.

Things had begun going awry when the city of Gnok's sanitation control center started directing its autonomous garbage trucks to random locations, none of which was a collection point. Too late, system operators realized something was wrong when electric trucks en-route to depots stopped dead in their tracks, blocking streets and intersections. Attempts to send troubleshooting teams were thwarted when they discovered their remaining fleet had drained batteries due to suspicious errors in their recharging systems. Pleas to borrow gas-powered vehicles from other departments fell on deaf ears; there were no longer enough to go around after the city allocated most transportation funds to autonomous systems. That is when they came to him for help. And that is when drones began raining explosives on his division's personnel carriers.

His intelligence officer initially suspected the traffic camera network had been hacked, enabling the drones to find–and strike–coalition vehicles with lethal precision. But even after he had made the call to shut it down, the attacks continued. Their next working hypothesis was that the enemy had compromised the 5G network somehow, using it to geolocate his troops. Consequently, the division took the city's wireless broadband offline as well, and with it the sensors monitoring

Lieutenant Colonel Robert J. Ross is the Information Warfare Team Lead in the Army Cyber Institute at the United States Military Academy (USMA) located at West Point, New York. Lieutenant Colonel Ross leads a 7-person, multi-disciplinary research team dedicated to expanding the Army and the nations body of knowledge on cyber and information-age conflict. He has a B.S. in Computer Science from Rowan University, an M.S. in Computer Science from Monmouth University, and a Ph.D. in Information Science from the Naval Postgraduate School. Additionally, Lieutenant Colonel Ross is an assistant professor in the Electrical Engineering and Computer Science Department at USMA, teaching primarily information technology courses. Lieutenant Colonel Ross' is currently a cyberwarfare officer and former artilleryman with two combat deployments to Iraq. His research interests are organizational science, strategic foresight, information warfare education, and digital economics.

and directing traffic. Gnok's streets were at a standstill, first responders were immobilized, and ongoing cyber-attacks were slowly degrading other essential services. Larsen contemplated a conundrum: "How is it possible to succeed in the physical occupation, while at the same time lose all control of the city? We are about to lose the people as well." A Smart City-led insurgency was the last thing he needed...

INTRODUCTION

Inter-connectivity is designed to increase the efficiency of city government operations and the quality of life for its citizens. It decreases costs and increases the municipal government's ability to efficiently manage the flow of traffic, control emissions, manage waste, and direct first responders. The goals of these, and many other Smart City initiatives, are to improve the quality of life for the city's residents, increase economic competitiveness, and achieve sustainability. The trade-offs for technologies that enable municipal digital transformations are the vulnerabilities that accompany any networked technology. Smart City technologies come with a panoply of vendors and other stakeholders, each with competing visions for the future. As the world becomes more urbanized and technologies become cheaper and more readily available, their use throughout cities in the industrialized and non-industrialized world will become more prevalent. The ramifications for military planning and operations increases in parallel. Smart Cities will become the status quo operating environment for urban military operations of the future. Occupying military forces will be responsible for the governance of these technologically controlled cities, particularly at the conclusion of large-scale military conventional operations (LSCO).[1] Future military forces must understand the implications for complex network ecosystems or risk ceding control over urban areas to the adversary during the return to competition phases of Multi-Domain Operations (MDO).[2] The

Greg Lindsay is a non-resident senior fellow of the Atlantic Council's Foresight, Strategy, and Risks Initiative, a senior fellow of MIT's Future Urban Collectives Lab, and director of applied research at NewCities. He speaks frequently about cities and technology, most recently at the United States Military Academy, Sandia National Laboratories, the U.K. Treasury, the OECD, Harvard Business School, and the MIT Media Lab. His writing has appeared in *The New York Times*, *The Wall Street Journal, The Atlantic*, *The New Republic*, and *World Economic Forum*, among many other publications.

Preface illustrates what could play out as a result of underestimating the impact of connected infrastructure during post-conflict operations in the networked urban environments of tomorrow. The scenario outlined above raises the specter of physically occupying urban terrain while losing control of the city.

Smart City initiatives are multiplying at an accelerated pace.[3] As of this writing, hundreds of Smart City pilot projects seek to make urban dwelling more sustainable by leveraging automation and digitizing interactions among technologies, people, and the physical environment. Each project is an ecosystem, with stakeholders ranging from government officials and technology firms with their near infinite supply chains to city residents. Many projects that began as experimental pilots are now integral to the way city government organizations deliver services to their constituents. Many more will follow.

An increasingly urbanized world, rapidly becoming more dependent upon technologies, adds ever greater complexities to future military operations. This article explores not only the implications these technologies will present to future military planners, but also proposes a framework for conducting joint intelligence preparation for military staff planning such operations in urban environments. Complex military operations begin with understanding the operational environment. The process by which the US military does this is the Joint Intelligence Preparation of the Operational Environment (JIPOE).[4] The complexity of digital ecosystems, their profound impact on city dwellers, and the potential opportunities and vulnerabilities they present to military commanders should be considered during that process. The authors propose here a framework that will enable the military intelligence community to begin designing a repeatable process to assess the Smart City environment and its impact on future military operations. More broadly, this framework can be used in the strategic planning process to aid in

identifying, visualizing, and communicating this information, and as a way to begin considering current gaps in military capabilities to disrupt, mitigate, or exploit these issues.

METHODOLOGY

The authors leveraged a combination of qualitative methodologies to identify key technological trends being adopted by municipal governments worldwide. Subsequently, the implications these technologies pose for future military operations in urban environments were derived. Three salient trends were identified after a comprehensive review of the literature on Smart City pilot projects implemented in urban areas throughout the world: autonomous mobility, machine-aided decision-making, and sustainability. These trends contained the primary data points to begin the process of Threatcasting, which is a strategic foresight methodology using narrative-building exercises dependent upon inputs from diverse groups of subject matter experts or knowledgeable agents.[5], [6] The contributing group was comprised of researchers with expertise in information warfare, cybersecurity, and urbanization. The Threatcasting process was used to derive several narratives describing a protagonist experiencing future threats, such as the one found in the Preface, after a series of remote and in-person interactions.

Threatcasting scenario modelling was conducted with the aid of a hypothetical adversary mission intended to influence the fictitious city government to withdraw from its security assistance agreement. The adversary sought to achieve its goals by disrupting government functions, eliminating the advantages of friendly exploitation of Smart City systems, and maintaining a foothold in these systems to retain the same advantages. This scenario was modelled to take place approximately ten years in the future. Each narrative derived from the scenario identified the importance for the adversary of keeping Smart City digital ecosystems operational to cause misattribution of violence and civilian suffering, and to discredit the occupying military force and host municipal government.

Upon completion of the narratives, the authors analyzed them using a methodology known as Thematic Analysis.[7] The Thematic Analysis process entailed decoding salient themes discovered within each of the narratives. Identifying the patterns of similar and dissimilar themes of each enabled the authors to identify inductively potential impacts of cyber-physical Smart City systems on urban military operations.[8] The combination of these qualitative methodologies was chosen as a method to provide description and a plausible explanation for the complexity that will be experienced by military forces operating in future urban environments.

SMART CITY TRENDS

The authors reviewed over 100 Smart City initiatives around the world, both past and present.[9] These initiatives, while interconnected in many ways, can be categorized as autonomous mobility, machine-aided decision making, and sustainability. These three technological

trends support the overarching goals and objectives of Smart City projects: sustainable urbanization, more efficient allocation of resources, and improved quality of life for city residents.

Autonomous Mobility

Municipal governments worldwide intend to use autonomous transportation to reduce congestion sharply and decrease private car ownership. By some estimates, driverless cars will quadruple today's highway capacity of 2,000 cars per lane per hour, to 8,000.[10] While the public trust in autonomous vehicles has declined due to recent fatalities, many cities worldwide are continuing to adopt technologies such as autonomous park shuttles and rail carriages.[11] As of this writing, over 70 global rail systems are equipped with trains capable of unattended operations such as closing doors, detecting obstacles, and reacting to emergencies.[12]

In the European Union, 47 participant organizations from academia, government, and the private sector deployed fleets of 10-passenger driverless vehicles in Italy, France, Switzerland, Finland, Greece, and Spain as part of a four-year, €15 million European Commission CITYMOBIL2 project.[13] In North America, New York City, Tampa, Ann Arbor, Columbus, and Las Vegas are testing vehicle-to-vehicle communications to enable building roads with built-in safety features. This technology connects vehicles to devices transmitting data about direction, speed, and location to roadside equipment, which sends it in turn to other vehicles, along with information from traffic light countdown, pedestrian presence, and cyclist sensors.[14]

Machine-Aided Decision-Making Affecting Changes in the Physical Environment

Advances in data collection, storage, and processing capabilities dramatically shorten the time between information inputs and decisions. The right data coupled with the right algorithm can help public officials gain insights into patterns of city-resident interactions and make decisions on improving infrastructure, optimizing the use of government resources, and enhancing public safety. Urban sustainability strategies outline objectives around more efficient sanitation management, energy utilization, traffic congestion, street parking, and other issues.

As an example, Milton Keynes' "data hub" was featured in the 2017 World Bank Internet of Things (IoT) report. Milton Keynes, a city in the United Kingdom with a population of 230,000, developed a central repository of data from an array of sensors, such as weather, traffic, lighting, trash bins, parking, satellite imagery, and air monitors.[15] The city made these data available via an application programming interface (API) to "inform analytics at different levels of detail to support intelligent planning and usage of resources across city systems."[16]

Another example is Barcelona, one of the "smartest" cities in Europe and host to the annual Smart City Expo World Congress. This city has implemented a range of systems affecting change in the physical environment based on sensor data. One example is a self-regulating park irrigation system that controls water delivery valves based on rain and humidity data. Another involves sensor-equipped trash bins able to detect weight and the presence of

hazardous materials, making collection more efficient.[17] Several international cities have installed under-asphalt weight sensors to guide city residents to open parking spaces. Yet another commonly adopted technology allows traffic lights to change their timing based on real-time traffic data.

Sustainability

Sustainability is an umbrella term encompassing a range of projects aimed at sustainable consumption of energy resources. These efforts include alternative energy production methods, zero-carbon initiatives, and energy conservation projects. Networked technologies that inform autonomous and human decision-making will continue to play a pivotal role in the success and sustainability of these projects.

The CELSIUS project, adopted by Genoa, Cologne, Gothenburg, Rotterdam, and Islington, uses systems that redeploy excess heat produced at commercial facilities, such as data centers, or extracted heat from sewage and biodegradable materials to heat residential facilities in high-density urban areas.[18]

The GrowSmarter project, piloted in Barcelona, Cologne, and Stockholm, aims to reduce energy consumption and green-gas emissions by 60% through a range of interconnected Smart City solutions, including waste heat recovery, smart street lighting, and smart mobility solutions.[19]

Smart City technologies supporting autonomous mobility, machine-aided decision making, and sustainability goals have the potential to greatly improve public service delivery, while presenting risks to rapidly degrade the quality of life for urban societies, particularly in the context of military operations. In a growing number of recent examples potentially debilitating cyberattacks have occurred against networked critical infrastructure. In the first widely reported attack against cyber-physical systems since Stuxnet, in 2017 a group of Russian hackers gained remote access to commonly used power equipment and shut down segments of Ukraine's power grid.[20] In April 2020, Iran attempted to penetrate Israel's water treatment facility "to mix chlorine or other chemicals into the water supply," resulting in the shutdown of agricultural pumps.[21] Sudden loss of critical services such as potable water and electrical power during stability operations are just two possible nightmare scenarios.

By the very nature of their functional requirements, Smart City devices are always on, continuously communicating with other system components. Their attack surface is always visible to malicious actors. Coupled with often poor situational awareness by owners and operators of these ecosystems, the sprawling attack surface provides ample opportunities for attackers to exploit these systems without notice.

Due to the relatively low opportunity cost, adversaries will continue attempting to exploit vulnerabilities in cyber-physical infrastructure to achieve their operational and strategic objectives, especially in situations where they lack conventional military advantage. Military forces conducting operations in future urban environments must identify and understand the

vulnerabilities inherent in Smart City technologies. Grasping the potential effects of adversaries exploiting these systems must occur during the planning phases prior to operations.

PLANNING CONSIDERATIONS

As the three trends outlined above materialize into everyday reality in cities, military planners will face increasing challenges if they misestimate role of digital ecosystems in supporting city life. As with any complex problem, it is helpful to break the problem down into components and visualize the relationships between those components.

Autonomous mobility, machine-aided decision-making, and sustainability are three functional categories introduced as salient Smart City trends discovered within the literature on urban pilot programs. Each category has been developed for a unique purpose; however, the components that comprise systems within each category have similar functional characteristics. At a minimum, the digital ecosystems comprising each category contains sensors that measure the current state of an object (e.g., temperature, weight, location, and velocity). Measurements obtained by sensors effect physical changes to an object's state (e.g., acceleration of a vehicle, turning a valve, changing the voltage in a power system) to achieve a desired end state. These same concepts are comparable to current industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems and are extended to other applications of Operational Technology (OT) and Industrial IoT devices.

OT networks composed of systems that communicate with each other, rather than with human users, must be viewed as a part of the convergent technology gestalt during planning considerations. Other intermediary components that facilitate the collection, processing, analysis, and transport of data from sensors to controllers and actuators will be introduced below. Smart City digital ecosystems are comprised of physical objects and digital devices that inform each other's state in a continuous cycle which is depicted in the Figure below.

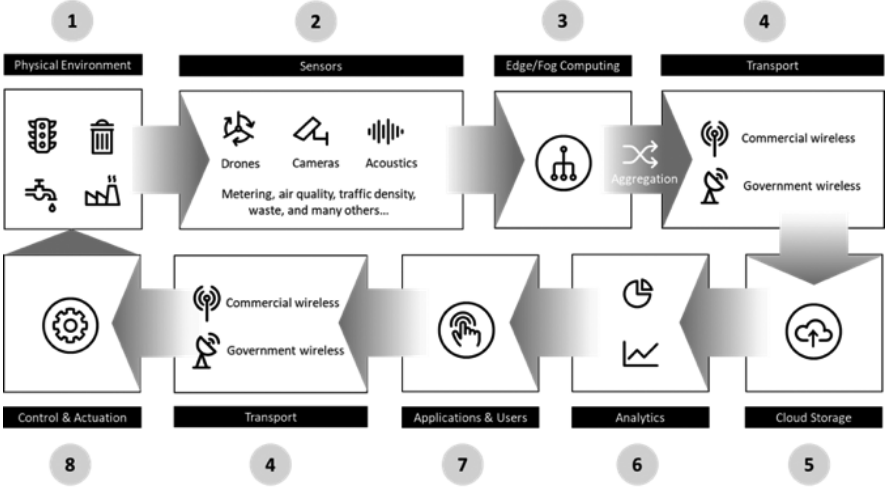

Figure 1: Common Smart City Ecosystem Components

The authors propose the following definitions for components depicted in the image above:

1. Physical environment contains physical objects that are affected by force applied to them through controllers and actuators for the purpose of changing their state.

2. Sensors measure the state of an object, convert analog measurement into digital signal, and transmit that signal over wires or a frequency within the radio spectrum. Data collected by the sensors may be transmitted to centralized computing and storage resources in the cloud or enterprise data centers, or to edge computing nodes for initial processing.

3. Edge computing systems collect digital signals near the source of the data, apply transformation to the data (e.g., selection of relevant fields or rearranging of fields into a common data model), and make decisions regarding which data should be sent further upstream (e.g., send to the cloud only data that indicate a change from the last known state). Fog computing extends cloud computing to the edge of the enterprise network decentralizing data processing activities across several local devices. As opposed to edge computing, which processes data on the sensor devices, fog computing places intelligence within processing hubs on the same local area network.

4. Data **transport** networks facilitate the transfer of data in real time from local devices to traditional data centers or the cloud. While the data can be transferred over the wire, wireless technologies play an increasingly central role in enabling the transfer of data from the enterprise network to the cloud. Furthermore, the rollout of 5G technology promises to provide the bandwidth, low latency, reliability, and increased network capacity required to accelerate adoption of Smart City technologies.[22] The features offered by 5G technology, particularly as they relate to mission-critical reliability, will extend the application of Industrial IoT use cases being piloted and adopted by cities worldwide.[23] Today, there are two primary operating models used to facilitate the transport of data: government wireless broadband networks (which may be owned and operated by a chain of private sector vendors and leased by the municipal government for its exclusive use), or commercial wireless broadband networks.

5. Remote **cloud** computing and storage facilitate the necessary on-demand elasticity and scalability to collect and process vast amounts of data from many millions of devices within a digital ecosystem. For the purpose of this analysis, storage and processing of data within data centers owned and operated by third-party providers present an additional layer of opportunity for attackers.

6. Analytics platforms, which may be extended components of the cloud computing platform or fourth-party Software-as-a-Service tools, filter and further transform the data, then stream them through an analysis engine to make decisions on the required alteration of an object's state. Analytics engines apply algorithms to data pre-processed at the edge to extract actionable insights within or across data sets.

7. Application is the layer where users of an ecosystem interact with its components. This layer may be used to customize analytic models, override or halt autonomous processes, or interact directly with controls and actuators. Autonomous OT operations are also configured and monitored at this layer.

8. Actuators change the state of physical objects by receiving digital signals over optical fiber, copper wire, or radio, converting digital signals into electrical pulses which excite physical objects into motion. Other types of **controllers** may change the display on a billboard or traffic signal, or input to another system.

During the planning process, the ecosystem components described above should be further decomposed into devices and nodes, with a mapping of interdependencies between the nodes. Each of those nodes should then be examined in the context of vulnerabilities or the opportunities it presents to both friendly and enemy forces.

Table 1: Operational Advantages and Effects

Component	Potential Operational Advantages	Enabling Effects
1. Physical Objects	• Remotely, controlled machinery supporting critical services—such as water treatment—may be physically destroyed in order to influence city residents' sentiment. • Delivery of power or connectivity may be disrupted or disabled to render physical objects inoperative.	• Physical Destruction • Disruption in Energy Supply or Communication
2. Sensors	• May provide additional intelligence, surveillance, and reconnaissance capabilities through legitimate or illegitimate access. • May be disabled through physical destruction or denial of service to counter adversary surveillance, or to disrupt government services. • May be used as nodes in covert mesh communication networks. • Sensors can be spoofed in order to transmit false data to computing devices.	• Physical Destruction • Endpoint Denial of Service • Device Spoofing
3. Edge Computing	• May be leveraged as data interception nodes. • Data altered at points of collection may result in misleading representation of ground truth. • May be used as entry points into upstream networks. • Traffic may be forwarded to unauthorized destination.	• Physical Destruction • Exfiltration • Transmitted Data Manipulation • Runtime Data Manipulation • Endpoint Denial of Service
4. Transport	• Capabilities can be integrated into Primary, Alternate, Contingency, Emergency (PACE) planning to augment limitations and vulnerabilities of line-of-sight and satellite radios. • May be used for device geolocation and precision physical and logical targeting.	• Physical Destruction • Exfiltration • Network Denial of Service
5. Cloud Storage	• Access to cloud-based services can be temporarily disabled through bandwidth or resource depletion denial of service attacks, causing disruption of government services during critical temporal junctures.	• Network Denial of Service • Stored Data Manipulation
6. Analytics	• Unauthorized access to analytics platforms allows altering decision algorithms, directing controls and actuators to effect desired change in the physical environment.	• Runtime Data Manipulation
7. Applications	• Access to applications can be denied at critical locations through application-level attacks. • Access to underlying data through application-level attacks can aid in surveillance and targeting efforts.	• Endpoint Denial of Service • Runtime Data Manipulation • Account Access Removal
8. Control/ Actuation	• May be used to effect changes in the physical environment at the device or remotely via ecosystem components. • Center of gravity in shaping attitudes of city residents about intention and competence of municipal government and foreign forces.	• Physical Destruction • Device Spoofing • Transmitted Data Manipulation

Table 1 represents common Smart City ecosystem components supporting any of the three functional categories—autonomous mobility, machine-aided decision making, and sustainability—and presents potential operational advantages provided to either friendly or adversary forces through legitimate or illegitimate access. The authors did not attempt to create a comprehensive list, instead depicting only some of the possible advantages and enabling effects. The planning process should reflect the current state of intelligent infrastructure within urban space specific of a particular environment.

PROPOSITIONS

Rapid urbanization and adoption of Smart City technologies are creating "conditions, circumstances, and influences" that will be exploited by future adversaries, particularly by militarily inferior state and non-state actors.[24] The Joint Intelligence Preparation of the Operating Environment (JIPOE) process requires joint force staff to define and describe the operating environments holistically using a systems perspective.[25] However, this macro-analytical process does not specifically account for the unique implications, cognitive and technical, posed by technologies that connect digital networks with the physical environment and exert an influence on the latter. The same is true on the micro-analytical level. While the U.S. Army's Intelligence Preparation of the Battlefield (IPB) process can be used to address informational and cognitive aspects of the operational environment, high-level cyberspace considerations are relegated to an appendix of the IPB application doctrine, and do not explicitly discuss implications for operating in digitally networked urban environments.[26]

The US military envisions the future operational environment as increasingly urbanized; however, the challenges anticipated with operating in that environment are primarily classified as physical and social, drawing on the lessons of recent conflicts in the Middle East.[27] A framework is urgently needed to layer understanding of rapid technological advances in the areas of autonomous mobility, machine-aided decision- making, and sustainability with military strategic planning.

The authors propose that military planners consider the following set of questions in order to understand the impact of Smart City infrastructure on future operations. These questions will help anticipate potential vulnerabilities in force protection, counterintelligence, and civil considerations, and aid in identifying opportunities for exploitation. More broadly, they can be used to formulate a framework for identifying, visualizing, and communicating this information as a way to begin considering—on a strategic level—current gaps in military capabilities to disrupt, mitigate, or exploit these issues, and developing solutions.

I. What are the essential government services that leverage technological advances in autonomous mobility, machine-aided decision making, and sustainability?

Planners should first identify services that are critical to the sustainment of life and safety of city residents. Next in order are services essential to the economic well-being of the city. Last

are services that aim to improve the quality of life for residents. Information should be collected on organizations and identities of "business owners" and stakeholders of essential services.

II. What are the components that make the delivery of those services possible?

Once services and their owners are identified, planners should identify the traversal path of the signal lifecycle, from sensor to actuator or controller for each essential service. This analysis will identify key technical components that make the delivery of a specific service possible. During this stage, technology owners of a given essential service should also be identified. These may be specific groups within the city's centralized Chief Technology Officer or Chief Information Officer functions, or within similar groups at organizations responsible for the delivery of services under consideration. At this level of analysis, the type of components represented in the table above should be identified and visualized.

III. What are the devices that make up components of the ecosystem?

High-level components are made up of physical devices that play a specific function in the signal's lifecycle. Planners should identify as many of those devices as feasible, including makes and models. To the extent possible, planners should identify parties responsible for operations and maintenance of those devices. These parties may be government employees, prime contract vendors, manufacturers, or any combination of the three. Network device tracking tools should be identified, and devices that make up the subcomponents of a given ecosystem should be mapped by authorized systems. Identification and monitoring of authorized devices prevent nefarious network devices from entering these networks.

IV. What are the interdependencies between essential services, their components, and devices?

The objective of this step is to map out the entire "system of ecosystems" with the aim of identifying technical interdependencies. It is becoming increasingly likely that data collected and processed by one city organization for the delivery of its service are being shared with another organization. A service of this second organization may use the first organization's data along with other data types to produce decisions supporting the delivery of that service. Interdependency analysis will identify system nodes of an even higher priority. Emerging technologies that aid in the discovery of system dependencies (through agentless collection and analysis of network packets, for example) should be utilized when feasible, and represented as visual graphs.

V. What are the supply chain dependencies within the digital ecosystem?

Supply chains supporting complex systems are becoming nearly infinite. Nevertheless, or perhaps because of it, the supply chain remains the threat vector of choice for advanced attackers. Supply chain analysis should include the identification of Industrial IoT vendors and their suppliers, mapped to system and device components and potential vulnerabilities in those components. It should also include the identification of the digital supply chain dependencies

such as code compilers.[28] Supply chain visibility is needed for increased vigilance, but most importantly for the city's reliance on those systems. While it is the city government's primary responsibility to identify supply chains and require primary contract vendors to conduct resilience and recovery exercises with their suppliers, military planners should map out supply chain dependencies to be able to support recovery operations as situations require.

VI. What operational and strategic advantages may be gained by friendly or adversary forces through legitimate or illegitimate access to ecosystem components and devices?

Given both the friendly and enemy missions with respect to a given urban environment, planners should consider how control of the digital ecosystems may assure or accelerate mission success. Further analysis in this step will identify components or devices that may facilitate this success. It is also important to consider during this step which components and devices, when subjected to degradation or destruction, may alter the lives of city residents significantly enough to delay mission fulfilment, or cause the tide to turn in another direction. Center of Gravity (COG) analysis may aid in the identification of cyber capabilities, requirements, and vulnerabilities that will yield the greatest operational gain.[29]

VII. What vulnerabilities are present in the devices that would allow the adversary to exploit them for their operational advantage?

Given the list of prioritized systems and devices, planners should identify Common Vulnerabilities and Exposures (CVEs) associated with those systems. Planners should also identify which systems are exposed to the Internet and conduct non-intrusive reconnaissance to assess the presence of those vulnerabilities within exposed systems. Adversary capabilities and intent to exploit those vulnerabilities in prioritized systems should also be assessed during this step.

VIII. What tactical effects should friendly or adversary forces seek to achieve to realize the operational or strategic advantages through legitimate or illegitimate access to ecosystem components and devices?

Cyber Operations Officers on the Joint Staff can help narrow down cyber effects that would enable friendly or adversary commanders to achieve operational or strategic advantages identified in the earlier phase of planning. While the U.S. Joint Cyberspace Operations doctrine lists cyber effects as secure, defend, exploit, and attack, it does not offer cyber planners at the operational level enough specificity to describe desired outcomes.[30] The authors suggest leveraging a commonly used taxonomy of adversarial behavior, such as MITRE ATT&CK framework.[31] The use of commonly accepted terminology will facilitate integration among military and civilian planners and operators, and cybersecurity researchers from both the public and private sectors.

- **Physical Destruction** of a device degrades or disables a service permanently.
- **Account Access Removal** impacts the availability of systems through the removal, locking or modification of user accounts.[32]

- **Endpoint Denial of Service** attack degrades the performance of a computing device through resource depletion, or causes a persistent crash condition.[33]
- **Network Denial of Service** attack degrades or blocks access to systems by users or other systems through network bandwidth depletion.[34]
- **Runtime Data Manipulation** modifies information displayed to users or transmitted to other systems in order to alter business processes and/or human or machine-based decision-making processes.[35]
- **Stored Data Manipulation** through inserting, deleting, or manipulating data at rest with the intent of altering business processes and/or human or machine-based decision-making processes.[36]
- **Transmitted Data Manipulation** through manipulation of data in transit to storage or other systems with the intent of altering business processes and/or human or machine-based decision-making processes.[37]
- **Exfiltration** is a category of techniques that facilitate the unauthorized transfer of data out of the target network or device.[38]
- **Device Spoofing** exploits trusted communications by inserting rogue devices into the network that masquerade as legitimate devices and introduce false and/or misleading signals into the system.

The eight questions above are tailored for military staffs preparing their forces to conduct urban operations. These questions are intended, until formally written into military doctrine, to supplement the intelligence preparation process. Understanding the effects of Smart City technologies and how adversaries will exploit them as a method for influencing local populations and governments within urban areas controlled by military forces is paramount for success in any future military operation. These questions are part of a continuous intelligence process that should last throughout the entirety of any operations within future urban environments. As the uncertainty about each question is reduced, the information will contribute to the joint force commander's (JFC) decision-making on how to react holistically in defending against the exploitation of these technologies, as well as the cognitive effects on local populations.

CONCLUSION

The threat effects experienced by Major General Larsen and his troops in the Preface of this article may have been disrupted or mitigated, or the division may have been prepared to recover from them, had the commander's staff planned using the supplemental questions proposed in this article during their intelligence preparations for operations in the fictional Smart City of Gnok. The Commander's Operations, Intelligence, Electronic Warfare, Cyber, and Information Operations staff answering these supplemental questions would have identified vulnerabilities in the city's digital infrastructure. With this knowledge the division would have the potential

to disrupt adversarial attempts to exploit these vulnerabilities or raise them as threats to the division's mission. Answering the supplemental questions during intelligence preparation and then wargaming against them during the division's military decision-making process (MDMP) would have provided Major General Larsen's division a far greater chance of success.

This article defined three key trends—autonomous mobility, machine-aided decision-making, and sustainability—affecting future military operations in urban environments. It defined a generalizable, yet complex, technical ecology and the nefarious implications they pose within the context of military operations. Finally, the article proposed eight questions that are intended to supplement and enhance current intelligence preparation doctrine found at the strategic, operational, and tactical levels of warfare. The answers to these proposed questions are intended to define how adversaries may exploit urban COG technologies, and thus affect the way in which commanders bring capabilities to bear in defending against these exploitive efforts during future military operations in urban environments.[39]

US military staff planners working for global combatant commands, in conjunction with our allies and strategic partners, should start preparing for this and similar scenarios now. They should start by identifying, collecting, and cataloguing Smart City technologies being adopted by major urban areas throughout the world in the form of a high-level running estimate. This information should be included in the updating and development of contingency plans for military operations in major urban areas throughout their areas of responsibility. Supplementing the current JIPOE process with the techniques proposed in this article will help develop understanding of, and forge relationships with, the relevant urban governments and their commercial industry partners managing Smart City technologies.

Once situational awareness—at a technical level—of Smart City ecosystems in major urban centers has been obtained, future research on this topic is needed to identify capability gaps in force structure, along with requirements to disrupt, mitigate, or exploit these issues during urban combat operations of the future.

ACKNOWLEDGEMENTS

The authors thank Colin Ahern (Deputy Chief Information Security Officer, City of New York) for contributions to this article and for providing insightful comments on early drafts of the manuscript.

NOTES

1. "Field Manual 3.0: Operations," (2017), 1-1.
2. "Training and Doctrine Command Pamphlet 525-3-1: The U.S. Army in Multi-Domain Operations 2028," Department of the Army (Washington, DC: U.S. Department of the Army 2018), iii.
3. "Smart Cities–Adoption of Future Technologies," *World Engineering Day* online, January 2020, https://worldengineeringday.net/wp-content/uploads/2020/03/Smart-City-IOT-WFEO-Version-1.pdf.
4. "Joint Publication 2-01.3: Joint Intelligence Preparation of the Operational Environment," United States, Joint Chiefs of Staff (2014).
5. Natalie Vanatta and Brian David Johnson, "Threatcasting: A framework and process to model future operating environments," *The Journal of Defense Modeling and Simulation* 16.1 (2019), 79-88.
6. Dennis A. Gioia, Kevin G. Corley, and Aimee L. Hamilton, "Seeking qualitative rigor in inductive research: Notes on the Gioia methodology," Organizational Research Methods 16.1 (2013), 15-31.
7. Richard E. Boyatzis, *Transforming qualitative information: Thematic analysis and code development* (Sage, 1998).
8. Kathy Charmaz, *Constructing grounded theory* (Sage, 2014).
9. "List of Smart City Projects," Nominet, October 10, 2018, https://www.nominet.uk/list-smart-city-projects/.
10. Emily Badger, "Pave Over the Subway? Cities Face Tough Bets on Driverless Cars," *The New York Times* online, July 20, 2018, https://www.nytimes.com/2018/07/20/upshot/driverless-cars-vs-transit-spending-cities.html.
11. "Ground Rapid Transit," Get There, accessed January 3, 2020, https://www.2getthere.eu/group-rapid-transit/.
12. Wikipedia, 2020, "List of Automated Train Systems," last modified December 31, 2019, https://en.wikipedia.org/wiki/List_of_automated_train_systems.
13. "Cities Demonstrating Cybernetic Mobility," European Commission CITYMOBIL2, accessed January 3, 2020, https://cordis.europa.eu/project/id/314190.
14. Andrew Macleod, "Autonomous Driving, Smart Cities and the New Mobility Future," Siemens, accessed January 3, 2020, https://www.techbriefs.com/autonomous-driving-smart-cities-and-the-new-mobility-future/file.
15. "Internet of Things. The New Government to Business Platform: A Review of Opportunities, Practices, and Challenges," The World Bank Group, 2017, http://documents.worldbank.org/curated/en/610081509689089303/pdf/120876-REVISED-WP-PUBLIC-Internet-of-Things-Report.pdf.
16. "MK Data Hub," MK: Smart, accessed on January 3, 2020, http://www.mksmart.org/data/.
17. "Seven Ways that Barcelona Is Leading the Smart City Revolution," *Edie Newsroom,* December 12, 2018, https://www.edie.net/news/7/Seven-ways-that-Barcelona-is-leading-the-smart-city-revolution/.
18. "CELSIUS: Combined Efficient Large Scale Integrated Urban Systems," EU Smart Cities Information System, accessed January 3, 2020, https://smartcities-infosystem.eu/sites-projects/projects/celsius.
19. "GrowSmarter: Transforming Cities for a Smart, Sustainable Europe," EU Smart Cities Information System, accessed January 3, 2020, https://smartcities-infosystem.eu/sites-projects/projects/growsmarter
20. Andy Greenberg, "'Crash Override': The Malware That Took Down a Power Grid," *The Wire* online, June 12, 2017, https://www.wired.com/story/crash-override-malware/.
21. "Cyber attacks again hit Israel's water system, shutting agricultural pumps," *Times of Israel* online, July 17, 2020, https://www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps/.
22. Sagar Paliwal, et al., "5G as the Principal Enabler Towards the Establishment of 'IoT' Society," paper presented at 2017 International Conference on I-SMAC, Palladam, India, February 10-11, 2017.
23. Liz Centoni, "How 5G Will Accelerate Industrial IoT," Cisco, October 17, 2019, https://blogs.cisco.com/news/how-5g-will-accelerate-industrial-iot.
24. "Joint Publication 2-01.3: Joint Intelligence Preparation of the Operational Environment," United States, Joint Chiefs of Staff (2014), I-1.
25. Ibid.
26. "Army Techniques Publication 2-01.3: Intelligence Preparation of the Battlefield," United States, Department of the Army (2019), Appendix D: IPB Cyberspace Considerations.
27. "TRADOC Pamphlet 525-92-1: The Changing Character of Warfare: The Urban Operational Environment," United States, Department of the Army (2020).

NOTES

28. Yong Kang, et al., "XcodeGhost: A New Breed Hits the US," FireEye Threat Research, November 3, 2015, https://www.fireeye.com/blog/threat-research/2015/11/xcodeghost_s_a_new.html.
29. Rock Stevens, Daniel Votipka, Elissa M Redmiles, Colin Ahern, Patrick Sweeney, and Michelle L Mazurek, "The battle for New York: A case study of applied digital threat modeling at the enterprise level," in 27th {USENIX} Security Symposium {USENIX} Security 18.
30. "Joint Publication 3-12: Cyberspace Operations," United States, Joint Chiefs of Staff (2018), II-5.
31. "MITRE ATT&CK Matrix™ for Enterprise," MITRE ATT&CK, last modified October 9, 2019, https://attack.mitre.org/matrices/enterprise/.
32. "MITRE ATT&CK Matrix™ for Enterprise: Impact Techniques," MITRE ATT&CK, last modified July 25, 2019, https://attack.mitre.org/tactics/TA0040/.
33. Ibid.
34. Ibid.
35. Ibid.
36. Ibid.
37. Ibid.
38. "MITRE ATT&CK Matrix™ for Enterprise: Exfiltration," MITRE ATT&CK, last modified July 19, 2019, https://attack.mitre.org/tactics/TA0010/.
39. "Joint Publication 2-01.3: Joint Intelligence Preparation of the Operational Environment," United States, Joint Chiefs of Staff (2014), I-1.