JUNE 2022

Allied Smart Cities

Sustainable, Socially Responsible, and Secure

By Matthew P. Goodman, Akhil Thadani, and Matthew Wayland

Executive Summary

"Smart cities" are both a focal point of the digital transformation of the global economy and a growing area of competition between the United States and China. To counteract China's first-mover advantage in this area, the CSIS Economics Program's Reconnecting Asia Project recommended in a March 2021 report, *Global Networks 2030*, that the United States and its allies promote a high-standard smart city model. This paper examines two constituent technologies that are foundational to this model—fiber-optic cables and artificial intelligence (AI). This paper also discusses a third cluster of technologies—quantum—that will likely play an important role in the evolution of smart cities. To aid U.S. and allied policymakers, this paper also offers recommendations on how to promote best governance practices and ensure that preferred technologies and standards for global smart cities prevail.

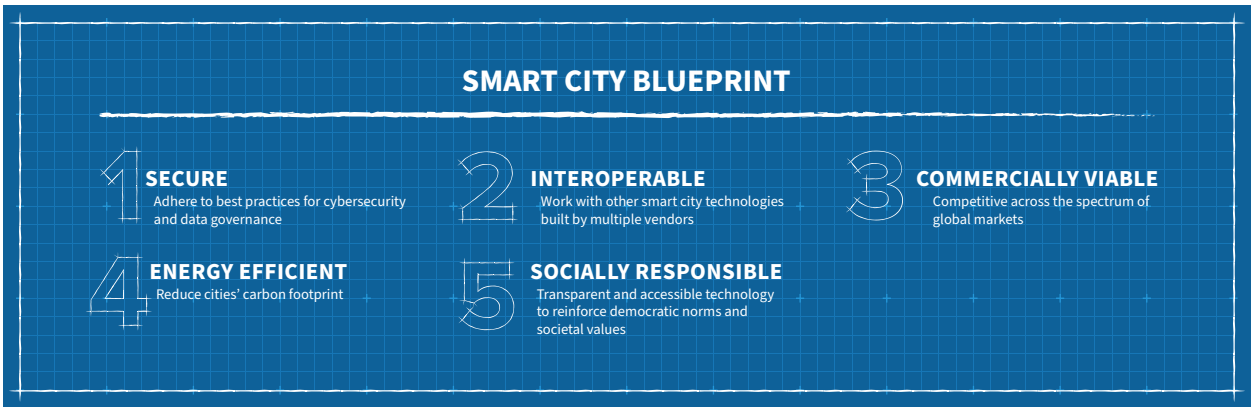
Introduction: The Stakes of Smart Cities

Population growth and rapid urbanization are reshaping global networks and driving demand for digital infrastructure beyond advanced economies. By 2030, 7 out of 10 people in the world will live in cities, and 96 percent of this urban growth will occur in less-developed countries in East Asia, South Asia, and Africa. These trends are accelerating U.S.-China commercial competition in third markets, where governments must decide which communication and technology governance systems to adopt. This competition has especially high stakes in the developing world, where there is enormous unmet need for connectivity solutions and Chinese firms have established a commanding position.

In densely populated areas, cheaper sensors, faster networks, and the proliferation of devices connected to the internet of things (IoT) can drive innovative solutions for long-standing urban problems such as traffic and pollution. Together, these technologies are the building blocks of "smart cities." Due to its origins as a commercial term, "smart city" has varied definitions. For the purposes of this paper, a smart city is a suite of urban technology systems that can gather and analyze data from sensors (often in real time), perform data-oriented decisionmaking, and shape policy outcomes.

Developing a high-standard smart city model can help to both successfully rejuvenate domestic infrastructure and close the global digital divide. The high-standard smart city (Figure 1) model must be commercially viable, energy efficient, socially responsible, secure, and interoperable. Digital technology impacts virtually all of the 17 UN Sustainable Development Goals (SDGs) and their 169 associated targets, which are intended to be achieved by 2030. SDGs relating to climate change mitigation are particularly vital for smart cities. According to UN Habitat, despite accounting for only 2 percent of the world's surface, cities consume 78 percent of the world's energy and produce more than 60 percent of greenhouse gas emissions.

Figure 1: Smart City Themes



Source: Authors' own analysis.

However, there are significant non-technical hurdles that stand in the way of employing emerging technologies to accomplish development goals. As many cities, even some in the United States, fail to provide basic services and infrastructure, a willingness to fundamentally change a city's policy approach is a prerequisite for adopting new digital systems. In the notorious case of contaminated tap water in Flint, Michigan, the decay of municipal infrastructure was not limited just to lead pipes. Years of budget cuts and emergency city management generated informational obstacles that bedeviled machine learning algorithms intended to solve Flint's water crisis. Additionally, ignoring the human element played by residents and municipal employees in rolling out smart city systems can exacerbate problems. City personnel must be trained to operate digital systems that collect sensitive, high-value data. To build out this capacity, bottlenecks in hiring due to civil service procedures must be removed.

The stakes are high. China is already advancing its own parallel vision for connectivity—the Digital Silk Road—and positioning itself to benefit strategically from the adoption of Chinese technology around the world. Led by national champions such as Huawei and Hikvision, China has built and implemented entire digital infrastructure systems in partner countries, potentially creating a dependency on a small set of vendors. Chinese companies have seen their market share swell by engaging markets that are underserved by other competitors and by offering products at a lower cost and with less hassle. Across Africa, Huawei alone is believed to have supplied roughly 70 percent of fourth-generation (4G) telecommunications networks.

Chinese firms have captured this first-mover advantage in exporting smart city technology by providing an attractive bundle of hard infrastructure and software services. Companies such as Huawei can offer a comprehensive smart city system—branded as "Safe Cities"—that promises to reduce crime and improve economic efficiency. Due to a lack of transparency and a willingness to work with unsavory governments,

China's global network ambitions are seeding techno-authoritarian norms and practices. Even countries that place a higher priority on privacy and data security, such as the United States, United Kingdom, and Japan, have purchased and installed elements of China's smart cities package. However, many Chinese smart city exports have faced technical and financial problems, which creates an opportunity for the United States and its leading technology firms to develop and export a higher-performing, values-driven alternative.

China's actions have started a ticking clock: without a coordinated response by the United States and its allies, effective global digital cooperation will be stymied. Leveraging bulk data collection through dominance of smart cities will enable China to shape global governance more effectively and alter public sentiment. Smart cities that are not interoperable with each other and lack common standards and values will accelerate the bifurcation of global networks, such as the internet, into separate spheres. In addition to its deleterious commercial and economic implications, this outcome would undermine U.S. national security and other interests by eroding liberal democratic norms.

COMPETING WITH CHINA

By some estimates, half of the world's smart cities are in China. This is no accident: Beijing has elevated smart cities to the level of a "national strategy" and treats their growth as a cornerstone of China's future economic and urban development plans. By promoting the development of smart cities internally, China developed hundreds of pilot projects that nurtured interlocking technology ecosystems through experimentation and refinement. In third markets, this gives Chinese firms—especially national champions Huawei, ZTE, and Hikvision—a leg up on the more distinct and disparate Western approaches.

In addition to the commercial challenges they pose, Chinese smart cities present substantial security-related concerns for the United States and its allies. The untrustworthiness of Huawei and ZTE systems in the eyes of Western governments has been clearly signaled. In addition, Chinese smart cities—while touted by Beijing as improving public welfare—are linked to intrusive surveillance programs, such as "Sharp Eyes." This has drawn particular attention in China's northwest province of Xinjiang, where smart city technologies such as biometric collection and facial recognition have been employed to identify, surveil, and detain the ethnic Uyghur minority population. Another concern is China's social credit system. While fragmented and dogged by implementation challenges, it is potentially a tool for mass surveillance and coercion if expanded and automated.

The Digital Silk Road has served as the international conduit for China's smart city exports, with the U.S.-China Economic and Security Review Commission identifying 398 instances of Chinese firms exporting smart city technologies in 106 different countries. Burkina Faso is a case study in how Chinese firms can package an attractive bundle of hardware and services to meet discrete needs. The Exim Bank of China financed a $94 million loan for the "Smart Burkina" plan, which deployed 650 kilometers of optical fiber built by the China International Telecommunication Construction Corporation (a subsidiary of state-owned enterprise China Telecom) and a Huawei-powered smart city system. To address growing violence, 900 surveillance cameras were installed to tackle urban crime and jihadist terrorism in Ouagadougou and Bobo-Dioulasso.

China's approach can be highly appealing to authoritarian regimes hoping to maintain their grip on power. In Zimbabwe, whose government has been ruled by one party since independence and which has long repressed opposition leaders and human rights activists, Huawei has installed a grid of public surveillance cameras for which Hikvision will provide facial recognition software. Such arrangements reveal the essence of the Chinese sales pitch: more options and quicker delivery with fewer conditions and less scrutiny.

Despite these concerns, the United States and its allies face huge challenges in rooting out embedded Chinese systems. "Rip-and-replace" of untrustworthy network infrastructure can be prohibitively

expensive, even for the United States, where Huawei and ZTE have made significant inroads in laying down telecommunications infrastructure in underserved rural areas. When Congress authorized a program to replace all ZTE and Huawei equipment already installed in U.S. networks, the Federal Communications Commission reported that $5.6 billion would be needed to reimburse providers (revised from an initial $1.9 billion estimate). In the United Kingdom, a similar "rip-and-replace" program is estimated to cost £2 billion ($2.6 billion) and will delay national fifth-generation telecommunications (5G) rollout by as many as three years. Therefore, after initial adoption of Chinese information and communications technology (ICT) equipment, countries may be locked in by exorbitant replacement costs that foster path dependency.

While China has built a significant first-mover edge, its missteps have left the door open for the United States and its allies. Evidence from smart city hubs in Kenya and Pakistan show crime rising and cameras malfunctioning. In Islamabad, murders, kidnappings, and burglaries all rose in 2018, despite Pakistan spending over $150 million on Huawei Safe City systems in 2016. An IT consultancy has accused Huawei of using their stolen software to establish a backdoor in the Lahore Safe City project, siphoning data important to Pakistan's national security and spying on Pakistani citizens. Chinese firms Hikvision, Dahua, and Uniview have all falsified tests required to export their products to South Korea. In short, leading U.S. companies can outcompete Chinese offerings if they increase their investment in overlooked third markets.

Three Key Technologies

Smart cities will be built atop of a large, dynamic ecosystem of different emerging technologies. Fiber optics and AI are notable components within the broader world of smart city technology that each have a separate set of considerations important to competing with China's smart cities initiative. As the backbone for other applications, the United States has a large commercial stake in ensuring that fiber-optic networks are open and interoperable, supporting competitive marketplaces and a plug-and-play model. For AI, the United States and key partners must define and implement values-driven approaches as automated systems are adopted in city infrastructure.

While it may not be top of mind for policymakers considering the nascent stage of development, there is substantial evidence that quantum technologies can help smart cities become more secure, efficient, and economically vibrant. Coupled with China's research and funding advantages in the sector, the potential civil and industrial applications of quantum technology mean that it also deserves robust strategic consideration.

TECHNOLOGY #1: FIBER OPTICS

Fiber-optic cables are bundled strands of glass—each about the diameter of a human hair—that transmit data in the form of signals by manipulating light particles (photons) over long distances. Fiber-optic cables serve as critical infrastructure and can be buried underground, submerged underwater, and hung from cell towers, connecting data centers, businesses, homes, and countries. Large networks of these cables make up the backbone of the internet, ICT, and smart city technology, providing the "pipes" through which data flows and playing a critical role in delivering broadband and 5G networks. Cable networks carry the majority of international data and are indispensable to the proper functioning of the high data throughput technologies that future smart city services will rely on. With minor adjustment, these cables are also able to function as sensors that collect information, gathering data to further smart city services.

The use of photonic technology in fiber optics provides key advantages over legacy systems such as copper wires that rely on electronic signals to function. Light moves extremely quickly, allowing fiber to deliver data at speeds of over 178 terabits per second—over a million times faster than the average U.S. household's internet speed. Compared to other forms of data delivery, fiber-optic cables also provide

lower latency—the delay experienced as data passes from one point to another—and less information loss and are up to 85 percent more energy efficient than copper wires.

As the demand for smart city solutions grows, so will the need for fiber optics; fiber-optic cables will provide the necessary underlying infrastructure for quantum networks and the vast amounts of data needed to feed complex AI models. Fiber optics will play a key enabling role in the development of smart city services. Current city-wide networks convert optical to electronic signals at several steps, using a mix of fiber optics, copper, and other types of network infrastructure. Smart cities will require energy-efficient, high-performance systems with ultra-low information loss and latency to support their constituent technologies, a challenge that legacy infrastructure is unable to meet. Moving to a truly optical network, or an all-photonics network, would entail using only light rather than electrical currents to transmit data at every step.

Fiber-optic networks will support several key services in smart cities. Three of the most important are broadband delivery, fiber-optic sensing, and providing the underlying infrastructure for other smart city services.

Fiber Optics for Broadband

The most widely impactful function of fiber-optic cables is providing broadband service. Internet delivery has undergone several evolutionary steps, with fiber-optic cables supplanting "cable" internet, which in turn replaced digital subscriber lines (DSL) and dial-up. As more developing countries come online, the world is experiencing an exponential growth in data demand, and internet access has become a critical necessity for participating in the global economy.

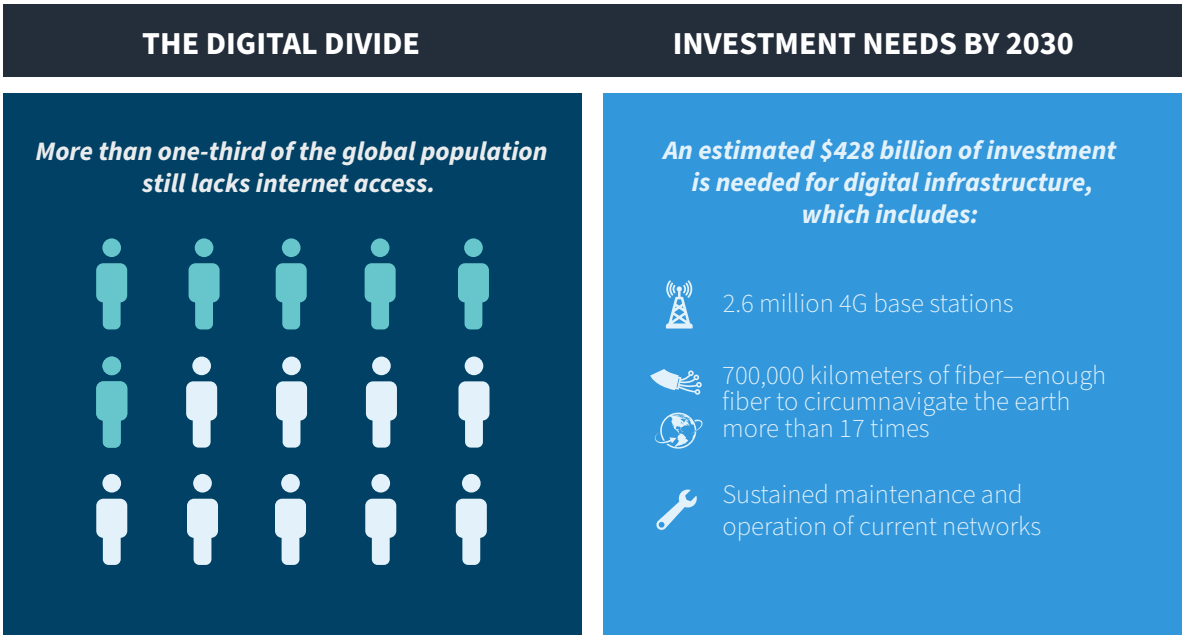
Despite its many advantages, fiber optics require large upfront investment to build. Laying down fiber-optic cables can be prohibitively expensive, especially in areas with irregular topology and low end-user density, such as rural settings. The U.S. Department of Transportation estimates that the average cost to deploy fiber-optic cables is around $27,000 per mile, with 90 percent of those costs originating from digging up roadways and burying the cable, not the cost of building the cable itself. For many cable builders, installing fiber networks is not profitable without a sufficient customer base to recuperate the installation costs.

Once an initial fiber-optic cable is built, internet service providers often route broadband to individual residential homes and businesses through less expensive and advanced delivery methods: DSL, wireless connection, or dial-up. The prohibitive costs of installing the "last mile" of fiber optics and broadband delivery poses a challenge to rural and broader regional integration. Without the existing market to justify the costs of expanding last-mile fiber optics, vast swaths of the population are denied access to the next generation of smart city technology. The challenge of rural and broader regional integration into the broadband network is critical for the expansion of future IoT services and the creation of "smart regions," as opposed to just smart cities.

Even in urban settings, simple access to a fiber-optic cable is not enough to ensure equitable broadband access. The United Nations International Telecommunication Union (ITU) estimates that the gap in internet users is six times larger than the gap in internet coverage. Likewise, rates of broadband adoption rest on factors other than the availability of fiber-optic cables. Wide adoption of broadband depends on users having the means to purchase internet services and the necessary hardware from which to access the internet, along with the technical literacy to navigate the internet. In the Central African Republic, for example, a month of internet access can cost consumers more than 1.5 times the country's annual per capita income. In New York City, a leader in smart city implementation, roughly 40 percent of residents do not have access to broadband despite widespread availability of fiber optics. The concept of smart cities rests on connected communities. Without affordable, quality access to the internet, there will be no users to support the market development of smart city services.

Low earth orbit (LEO) satellites, championed by companies such as OneWeb and SpaceX, are the next advancement in broadband delivery that is closest to market implementation. While LEO satellites—the subject

Figure 2: Closing the Digital Divide



Source: International Telecommunication Union, *Measuring Digital Development Facts and Figures 2021* (Geneva: International Telecommunication Union, 2020), 10, https://www.itu.int/en/ITUD/Statistics/Documents/facts/FactsFigures2021.pdf; United Nations Conference on Trade and Development (UNCTAD), *Digital Economy Report 2019* (New York: United Nations, 2019), 12, https://unctad.org/system/files/official-document/der2019_en.pdf

of a forthcoming CSIS brief—have the potential to reduce cities' reliance on fiber-optic networks, it is more likely that the two will work in tandem to bridge the global gap in internet delivery. LEO satellites will function better in remote areas and in difficult terrain, but the advantages of fiber optics in cost and performance make it difficult to imagine a future where satellite links wholly replace optical links.

Fiber-Optic Sensing

An essential function of a smart city is the collection of data to feed analytics and inform real-time decisionmaking. Sensors will be at the heart of that collection effort. Fiber-optics provide a cheap, energy-efficient, and privacy-preserving solution through fiber-optic sensing (FOS). FOS uses the physical properties of photons as they travel along an optical fiber to detect changes in temperature, pressure, displacement, and other parameters. Plugging an interrogator—an AI-enabled data collection terminal—into an optical fiber can transform one cable into thousands of sensors. FOS uses the cable itself as the sensing element, allowing real-time, continuous monitoring of the cable's surrounding environment.

FOS can be used for several smart city applications, including infrastructure and transportation monitoring, environmental measurements, and applications in healthcare. The technology is already widely accepted in the oil and gas industry, where fiber optics are used to monitor pressure and temperature along pipelines for preventative leak detection and pipeline flow rate measurement. Rather than waiting for an inspection truck to drive alongside a pipeline to detect any damage, sensors notify repair crews in real time, minimizing repair costs and environmental damage.

FOS provides distinct advantages in cost, energy consumption, quality, and privacy over other sensing technologies. FOS does not interfere with the regular functions of a fiber-optic cable, allowing for simultaneous broadband delivery and sensing. The complexity and cost of such a system is low since it uses preexisting infrastructure and requires little additional equipment, making FOS a commercially viable solution to a large portion of a smart city's data collection needs. Fiber-optic sensors do not need electricity to function, dramatically reducing the energy consumption to solely the needs of the interrogator. Continuous monitoring of information along the length of the fiber line provides deeper insights into the environment than other legacy technology that is limited to collecting information along critical points. Counties in California have used FOS to combat climate events by monitoring water levels during droughts and modeling seismic activity. Data collected by the continuous fiber along California's fault lines filled the substantial data gaps left by legacy sensors, which were often separated by 20 miles or more. Lastly, FOS's technical design allows it to collect only non-identifiable environmental data, mitigating privacy concerns about the collection of personally identifiable information.

Fiber as the Backbone of Smart City Technology

Fiber optics play a key enabling role in other smart city and telecoms technologies. The successful implementation of 5G networks, smart city sensors, and applications is dependent on a network infrastructure capable of supporting billions of devices and the large amounts of data they produce. The many advantages of fiber optics—from almost unlimited bandwidth potential and immunity from electromagnetic interference to lower latency—are critical to unlocking the benefits of 5G and broader smart city integration.

Fiber-optic cable networks will undergo expansion across metro areas as the demand for broadband and fiber-based services continues to grow. Specialized optical fibers are used for different applications, altering the shape and number of the cable's internal glass strands to optimize performance. These cables will need to be built with interoperability in mind, supporting the transition between optical and electronic signals as well as different types of optical equipment. Maintaining interoperability between the cables and their connectors built by different vendors is necessary to support a "plug-and-play" model for current and future smart city technologies. Ensuring network interoperability also reduces reliance on single vendors, allowing governments to avoid lock-in and the high costs associated with ripping up and replacing fiber-optic cables when new vendors offer competitive, trustworthy alternatives.

Once cable lines are built, cable operators can, in some circumstances, retain exclusive rights over which service providers have access to fiber optics, either through company policy or technical design. Maintaining an open access policy for publicly funded optical fiber networks would remove a cable operator's monopoly on who is allowed to "plug in" and use the network, ensure the network's status as public infrastructure, and foster a competitive and market-oriented environment for smart city applications that rely on fiber-optic availability. It would also ensure that U.S. and allied providers can better compete with companies such as Huawei, who position themselves as a one-stop-shop solution.

TECHNOLOGY #2: ARTIFICIAL INTELLIGENCE

Broadly defined, AI is a set of algorithms or automated rules that can process information, often in real time, to make decisions and perform actions. While fiber-optic cables connect end points in a city and quantum technology will fuel the services and applications that rest on the fiber network, AI will influence the flow and form of data through city infrastructure. AI models will help shape what data is collected and how it is stored, organized, processed, translated, and governed. As the volume and quality of data generated by a city grows, AI will help sort, process, and operationalize the information collected to aid municipal decisionmakers in reaching policy goals.

AI's use in city planning and services will have wide-ranging implications and the potential to shape how stakeholders—from municipal officials to citizens—think and act. AI's expansive role in smart cities already impacts outcomes such as which schools a person is admitted to, what areas or neighborhoods are surveilled more, or who is approved for a bank loan. While AI will automate several tasks in a smart city, it does not remove humans from the equation; the contexts in which humans place AI and how humans interact with AI systems will determine the technology's efficacy and ethical implications. Deciding where and how to implement AI in smart city infrastructure both face different considerations and do not necessarily share the same risks. These decisions will depend, in large part, on local governments' policy priorities, risk tolerance, and other values-based considerations.

Under the auspices of smart city projects, AI can play a key role in advancing authoritarian government control by promoting censorship, control over digital media and communication networks, and mass surveillance. In 2018, Venezuela debuted smart ID cards that, with the help of ZTE, a Chinese firm, track citizen political affiliation, voting records, and other behavioral information through an AI-enabled "fatherland database." Huawei, which is both China's largest telecoms company and its largest AI company, is responsible for exporting AI surveillance technology to at least 50 countries worldwide. Media sources have also uncovered specific cases of Huawei technicians working directly with government security forces in Uganda and Serbia—countries with dubious human rights records—to install surveillance technology and spy on political opponents.

Ensuring that AI-enabled decisions are made in an ethical manner consistent with democratic and broader societal values has already proved to be a barrier to wide adoption of the technology. Automation exists in context, with ethical considerations varying widely by use case, political structure, and the humans that control and work with it. Maximizing transparency, "explainability," accountability, and accuracy in AI will be key to ensuring the ethical application of AI systems.

AI Applications

AI, like all classes of technology, is better suited to certain applications than others. AI's ability to digest and translate large amounts of data lends itself to solving optimization problems and can be used to further broader policy goals. Allocating resources, minimizing loss, and increasing process efficiency are areas where AI reasoning exceeds individual human capacity; the use of AI to augment other technologies in optimizing energy and traffic management, for example, will further climate and safety goals. AI is already being rolled out in critical areas of city infrastructure and services, impacting how homes are powered, how people travel, and how people are governed. AI networks will be positioned such that algorithms have the potential to impact democratic values such as freedom, transparency, and equality. Municipal leaders will face different challenges in deciding *where* and *how* to adopt AI in city infrastructure.

As the renewable energy transition accelerates, power sources will become more diversified, requiring precise balancing to match supply and demand for energy without overloading a city's energy grid. In addition to coordinating energy flow, AI can be used to optimize power yield and predict power loads for more precise forecasting throughout energy grids, reducing costs for consumers, increasing performance for operators, and furthering UN climate goals. Some forecasts predict that "smart grids" will be where most spending on smart city applications is directed over the next five years.

AI, in conjunction with sensors and other smart city technology, can be used to coordinate traffic flows based on real-time data to reduce congestion and increase safety and mobility. Hangzhou, a Chinese city, managed to reduce traffic jams by 15 percent after introducing smart traffic monitoring in partnership with Alibaba.

When carefully and deliberately balanced with concerns over privacy and civil liberties, AI also has the potential to improve public safety and criminal justice outcomes. Predictive tools and real-time monitoring

enabled by AI can support emergency response teams and law enforcement officers. For example, traffic flow monitoring can help identify the quickest and least congested route for an ambulance. Studies show that the use of surveillance cameras, particularly in city centers, has the potential to reduce planned crime by up to 25 percent.

In the past, local governments around the world have rarely been able to effectively manage the trade-offs between AI implementation, privacy, and civil liberties. For example, using pre-trial algorithms as a risk assessment tool, based on past convictions and behavior, has helped judges determine how likely defendants are to skip court. This effectively allowed certain U.S. states to end cash bail, getting rid of a system that overtly disadvantages impoverished communities. However, these algorithms are far from optimal and have been found to not meaningfully reduce the disparities that have plagued older systems. To ensure efficacy and to minimize unintended consequences, city planners will need to take extra precaution when automating public safety applications through regulation and measured application of AI technology. In many cases, especially those related to using AI for public safety, this cannot be accomplished without addressing underlying policy-related issues outside of the scope of AI.

Ethical Challenges

Harm and risk reduction in implementing AI in smart cities requires taking ethical concerns into consideration when building and operating AI systems.

- **Bias in AI models:** Bias resulting from how AI models are programmed and trained is well explored. One of the earliest cases where machine bias was documented was in 1979, when an English medical school implemented an algorithm to help make the admissions process fairer and more efficient. The UK Commission for Racial Equity later found that the algorithm docked significant points off female and non-European candidates, reducing the diversity of the admitted class.

  The increased use of algorithms in public infrastructure and services has the potential to disadvantage far more people. One potential source for introducing bias in algorithms—the rules AI follows when performing its programmed function—comes from how algorithmic models are designed or trained. Machine learning (ML), a sub-class of AI, uses data to hone its predictive capabilities. ML models fed with inaccurate and nonrepresentative data will produce inaccurate and biased results. Because of this, trained ML models are context specific. A model used in and trained by data from New York will not necessarily function as well if used in Singapore.

  Controlling for bias in AI decisionmaking and predictions requires attention beyond how models are designed and trained; in cases where current policies and processes are racially biased or otherwise unethical, using AI to automate these policies and processes is likely to continue producing unethical outcomes, potentially at greater speed and scale or reduced cost. AI is a tool, and just as a car or streetlight cannot be made inherently ethical, examining how and in which contexts AI is used is necessary to account for unwanted outcomes. How the data and insights gleaned from AI are interpreted and operationalized depends on human understanding and is subject to human biases.

  Beyond the individual level, systemic bias results from how institutional design inherently disadvantages certain groups or ideas, not as the result of any conscious action but through existing rules and norms. Placing AI in contexts that suffer from systemic bias will reinforce biased outcomes. For example, while facial recognition software using AI has proved to produce inaccurate results when attempting to classify faces of color, even accurate facial recognition software will engender biased results if placed in a criminal justice system that overly surveils certain groups. AI adoption presents an opportunity as a good systemic transition point that would prompt municipal leaders to consider the types of outcomes sought from upgrading city infrastructure. Overhauling city services to reduce

human and systemic bias through policy reform is necessary preparation for the equitable and ethical implementation of smart city AI.

Maximizing trust in automated systems requires pulling back the curtain on the black box of AI decisionmaking. Algorithms in use for public services are complex and often use large and incomplete data to function. How an AI model arrives at the decisions and conclusions it outputs is not easily decipherable to those not intimately familiar with the technical design of the specific model in question. Implementing mechanisms to explain AI decisionmaking and increasing transparency will improve accountability.

- **Privacy and AI:** The collection of massive amounts of data is key to building a smart city. Over the last decade, urban surveillance has grown into a multi-billion-dollar industry, with key U.S. and Chinese companies leading the way. However, collecting and operationalizing data brings with it a whole host of privacy and surveillance concerns, making it difficult for citizens to control who uses their data and how it is used. AI, when used contrary to democratic norms, has the potential to reinforce authoritarian regimes through increased surveillance, enabling government monitoring of everything from online behavior and location tracking to spending habits.

  The risk of surveillance is compounded by the proliferation of automated public services that would make it prohibitively costly for citizens to not offer up their personal data in exchange for participation. Location services that track where and when a person travels are incredibly useful to city planners for urban planning. They are necessary for services such as cellular calls, ridesharing, GPS route planning, and real-time traffic management. Moving through urban environments without location services enabled is increasingly difficult. For those on the other side of the digital and economic divide without the means to purchase hardware, such as a smart phone, and internet services through which to access smart city services, digitized public infrastructure could be out of reach entirely.

  Smart city applications threaded through public infrastructure that collect data can also make it impossible for citizens to opt out of data collection. London has installed over 600,000 facial recognition-enabled CCTV cameras in public spaces around the city, a number that is rare outside cities in China. For Londoners, surveillance is a fact of life. While the United Kingdom has legal protections such as stringent regulations on facial recognition that limit the use of CCTV data, the inability to reasonably opt out of data collection in other countries where democratic norms are less established has serious implications for civil liberties. London, as well as the recent example of using facial recognition to identify fallen Ukrainian soldiers, highlights the fact that the downsides and potential risks over choosing where to adopt AI are not necessarily the same as poor implementation of AI in chosen areas.

- **Implementation and privatization:** As automation is increasingly rolled out in public services, governments that lack the expertise and capital to hire in-house AI engineers often contract out the work to private companies. Privately developed algorithms and models are being used to shape government actions in critical areas such as criminal justice, energy management, transportation, and food safety, which raises multiheaded concerns for ethical implementation. How algorithms are built and trained is often removed from public oversight. Government officials, the vast majority of whom are not technical experts, will need to understand and explain the systems they use in order to account for the decisions made based on those systems. Transparent AI would require knowledge over the assumptions and data that underpin an AI model's decisionmaking, which puts pressure on private companies seeking to avoid publicizing confidential and proprietary information. Public-private partnerships also

raise questions over the commercialization of public data and data collection in city spaces. Safeguards to preserve public interests in AI implementation will need to be addressed through changes to policy, such as a city's procurement process, in order to be effective.

City planners will also need to address concerns over redundancy in performance and protection of personally identifiable data when implementing AI in smart city services. Increasing reliance on automated systems for public services may widen gaps in human involvement. In the case of outages or circumstances in which it is not optimal to use AI, building safeguards for retaining human capacity and creating redundant contingencies becomes critical for key city services.

AI Governance in Cities

There is a tendency to fall back on overly technical solutions when attempting to solve for ethical concerns and governance challenges in smart city AI. Integrating AI into city services while accounting for shared democratic values requires deeper insight into the context of its use and realignment of policy sometimes completely unrelated to the technology in question. Officials in New York found pension policy to be an unexpected challenge when attempting to operationalize AI in city services. Hiring AI experts is extremely costly and pension requirements for public employees are stringent, making it too expensive to realistically build a municipal workforce capable of bridging the gap between technical and policy considerations.

As cities continue to embrace automation in services, certain countries such as Japan have taken a "soft law" approach to AI regulation. Soft laws are non-enforceable but substantive standards and best practices to guide the use of certain technologies, allowing for flexibility in regulation. Development of AI technology far outpaces even the most zealous regulatory bodies, and retaining a soft law approach keeps unnecessarily constraining and outdated regulation from hindering progress or performance.

In an attempt to preserve privacy and halt AI's potential infringement on civil liberties, San Francisco banned facial recognition from use in city departments. While hailed as a model for privacy-preserving legislation, city officials and key watchdog organizations have argued for broadening exceptions to allow for limited use of the technology to combat rising crime. Many smart city facial recognition technologies sold today suffer from serious problems of accuracy and bias that should not be ignored; however, taking a more fine-grained approach would allow for its productive use while controlling for negative externalities. Facial recognition performance rests on the data that the AI is fed, the quality of sensors used, and the operational conditions—light levels or the distance from the target—in which it is placed. Government officials will need the time and expertise to make smart decisions on where and how to implement AI technology in cities.

There is no shortage of organizational AI governance frameworks, principles, and guidelines. The European Union, the U.S. National Institute of Standards and Technology (NIST), the Organization for Economic Cooperation and Development, and others are developing risk-based frameworks that guide implementation by classifying the threats posed to democratic values by automation. This approach helps retain flexibility in where and how regulations are applied while helping local officials learn how to think and identify threats in smart city AI. Attempts at AI governance in cities will need to address the underlying policy considerations, unrelated to the technology, that hamper AI deployment to sufficiently prepare municipalities before grafting the technology onto public services and infrastructure.

TECHNOLOGY #3: QUANTUM

Quantum information science and technology (QIST) takes advantage of how physics operates on a small scale to enable transformational new capabilities. Quantum technology specifically refers to the practical application of quantum physics in useful devices or algorithms. While they may seem abstract, insights

about quantum mechanics like superposition and entanglement facilitated the development of now ubiquitous technologies such as transistors, lasers, and MRI scanners.

A major obstacle to the development of useful quantum applications is the lack of targeted government funding. In the United States, research and development (R&D) funding is primarily private sector driven, reflecting the vibrancy of the U.S. venture capital ecosystem. Yet, it is still too early to assess how successful these start-ups will be at fielding viable products. Relying only on the marketplace also heightens the risk of a "quantum winter" scenario, where high-profile quantum start-ups fail to meet outsized expectations and dampen investor interest in the sector. This outcome also has strategic implications, as companies with large market shares will play outsized roles in writing standards and establishing norms of how the technology will be used, as evidenced by Chinese firms such as Huawei and ZTE leading the development of 5G wireless standards.

In terms of total historic announced public funding for quantum, the United States ($1.2 billion) decisively trails both the European Union ($7.2 billion) and China ($15 billion), where research concentrated in government labs has demonstrated rapid technical progress. This gap could be narrowed by the passage of the United States Innovation and Competition Act, which allocates $110 billion for general research funding and emphasizes the development and standardization of quantum technologies. The bill passed the U.S. Senate with strong bipartisan support and is currently pending reconciliation with the House of Representative's America COMPETES Act.

Increased funding could accelerate the development of two quantum applications that will impact smart cities: quantum-based-sensors and quantum communications.

Quantum-Based Sensors

Quantum-based sensors (QS) can detect minute changes in the environment to carry out measurements of physical quantities that are 1,000 times more precise than ordinary sensors. The first generation of quantum sensors includes devices like microwave atomic clocks. The second generation of quantum sensors is now emerging and will enable higher-precision measurements of gravity, temperature, air movement, and magnetic fields based on ultra-cold photons. QS will be able to measure data that cannot be captured by current sensors, which are either too large or lack the required functionality. They can provide a number of advantages for smart city infrastructure:

- Quantum gravity sensors can identify geophysical targets in civil engineering, such as buried utilities, sinkholes, and mineshafts with a higher degree of precision. This can reduce health and safety risks and decrease the cost of road and subway repairs. UK-based researchers have opened a commercial pathway by demonstrating the use of this technology in real-world conditions.

- Considering the vulnerabilities of GPS, QS can increase the reliability and resiliency of satellite-based navigation systems. QS can make navigation available in places without satellite coverage, such as underground tunnels, or when a signal has been deliberately or accidentally scrambled.

- More highly calibrated light detection and ranging (lidar) will assist with the control and navigation of autonomous vehicles as they round corners.

- Quantum-enabled radar has the potential to improve the capabilities of conventional radar to detect smaller targets such as drones and birds. Identifying these targets can mitigate threats to airports and other city infrastructure.

Despite this promising range of use cases, commercialization and integration hinges on the development of miniaturized hardware that can be deployed outside of laboratories. This is particularly challenging

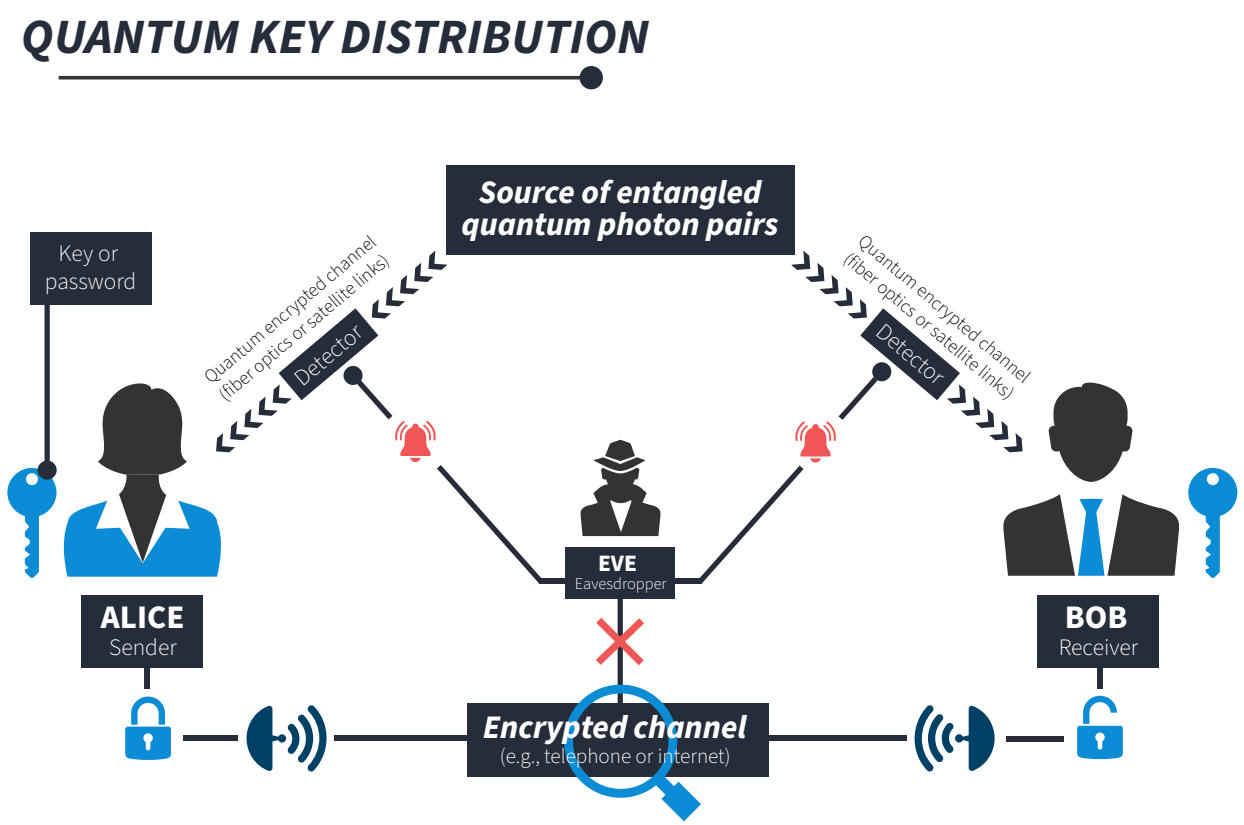
because quantum systems are so fragile, leaving QS highly susceptible to noise in the form of interference from the surrounding environment. If these engineering challenges can be overcome, more fiber-optic networks will be needed to support widespread quantum sensors, as fiber cables are capable of providing a cold stable environment with low information loss for transmitting photons.

Quantum Communications

The most trenchant security issue concerning QIST has long been understood: a fully functional quantum computer could rapidly crack messages encrypted with the widely used RSA encryption algorithm. Quantum communications (QComm) involves encoding and transmitting data in a manner that is "unhackable" even by quantum computers. QComm can be used to protect data in the finance, defense, utilities, and heath sectors as well as the critical infrastructure that underpins smart cities and energy grids.

Presently, quantum key distribution (QKD) is the most popular method of quantum transmission and works by encoding each bit of the cryptography key on a single photon. As depicted in Figure 3, if an eavesdropper attempts to read or intercept the transmission, the information encoded on the photon will be lost and the attempted interception will be observable, alerting the communicating parties to the interference. Unlike other quantum applications, QKD has demonstrated commercial uses—such as securing J.P. Morgan's peer-to-peer blockchain banking network—and has proven to be high-speed, stable, and interoperable at short distances.

Figure 3: Quantum Key Distribution



Source: Adiyita Jami and Shankar Rao Priya, "Quantum Cryptography," Andhra University, https://cs.stanford.edu/people/adityaj/QuantumCryptography.pdf.

Facilitating transmission of QKD over longer distances is a major operational challenge and will not be feasible until researchers are able to build fully functional quantum repeaters. Without repeaters—devices that amplify signals and reduce the amount of information lost during transmission—Qcomm can only be carried out between "trusted nodes," intermediaries that decrypt and re-encrypt keys to extend the key transfer distance. For long-range transmissions, Qcomm may rely on satellites both to defray the cost of long optical cables and because even in optical fibers, photons are lost to noise within a few hundred kilometers.

While the United States remains the global leader in most quantum technologies, U.S. R&D in Qcomm remains primarily academic, and thus the United States lags far behind China in deployment. China launched the world's first quantum-compatible satellite (Micius) in 2016 and is the only nation to demonstrate key enabling steps toward long-distance quantum networking, achieving QKD over a total distance of 4,600 kilometers with a mix of satellite and ground nodes. This "Sputnik moment" prompted U.S. policymakers to fund the National Quantum Initiative, including the Department of Energy's efforts to build its own quantum internet. China has also been active outside of military and academic spheres in Qcomm, with some users of China Telecom, one of China's "Big Three" telecom companies, able to make quantum encrypted phone calls as part of a pilot test started in Anhui Province, though details about this program are scarce.

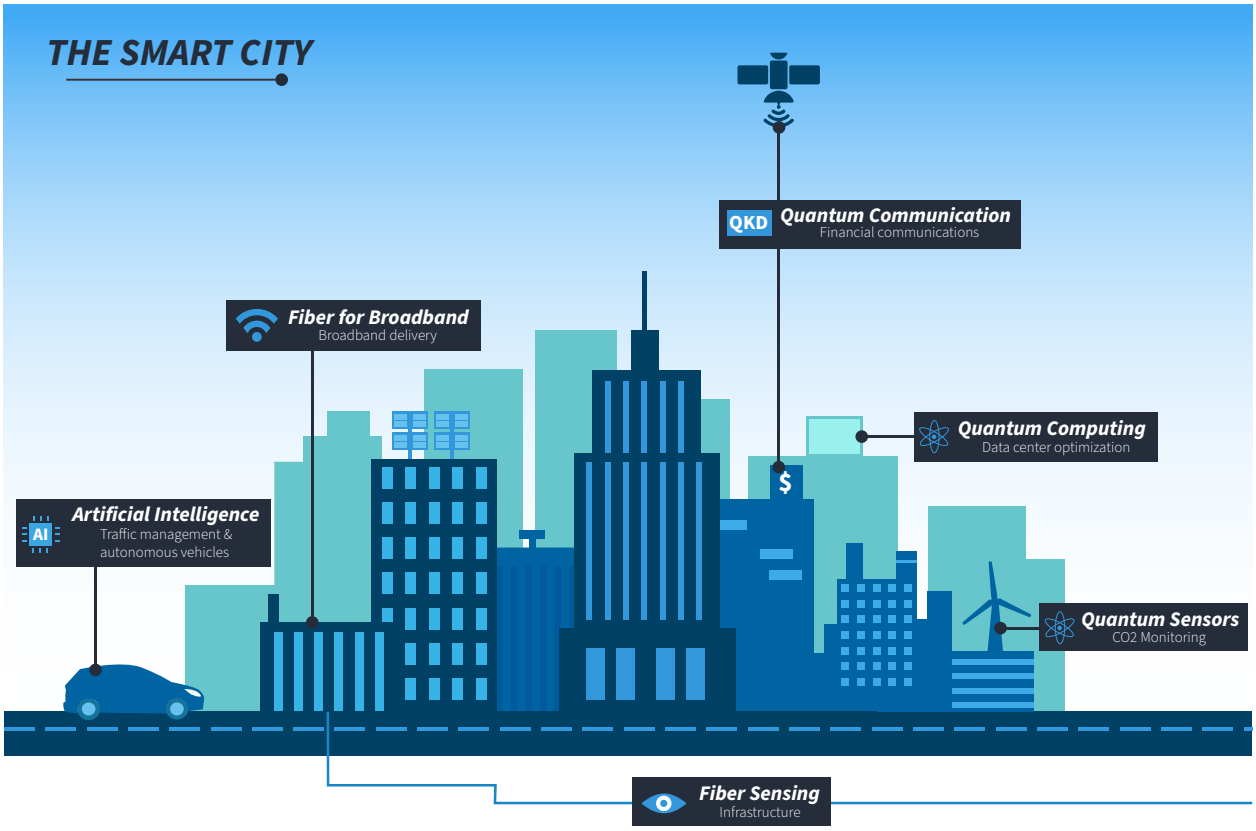
Securitization of Quantum

A major challenge is securing quantum from illicit technology transfer while still promoting open scientific research. Recent policy moves (by both the United States and China) have erred on the side of restricting trade in quantum technology due to its potential military applications. "Quantum sensing and information" is one of the 14 emerging technologies identified by the Department of Commerce for export controls. In November 2021, the Department of Commerce added eight Chinese quantum computing companies to the Entity List. As a response to U.S. restrictions, China launched its own industry panel called the "Xinchuang Committee," which has drafted import controls to block technology companies that are more than 25 percent foreign owned from supplying sensitive industries.

The emphasis on security in the quantum sector could come at the expense of allied collaboration. One positive exception is the Tokyo Statement, signed in 2019, which represents a commitment between the United States and Japan to cooperatively advance values-driven quantum technology by promoting freedom of inquiry, research rigor, intellectual property protection, transparency, and accountability, among other values. On the multilateral level, some encouraging work has already been done to develop international standards for quantum technology and stimulate their commercialization. In the ITU, standardization work is addressing network and security aspects of quantum information technologies with an initial focus on QKD. The Institute of Electrical and Electronics Engineers (IEEE) has developed a platform to engage the quantum research and business communities.

While many of these issues are being determined nationally or in multilateral fora, it is important to initiate conversations about cybersecurity at the city level, as local actors need to be especially proactive about preparing for a transition to post-quantum cryptography (PQC). Smart cities will have growing attack surfaces as more systems are brought online, and their decisionmakers should be closely monitoring NISTS's ongoing PQC standardization process.

Figure 4: Examples of AI, Fiber, and Quantum in a Smart City



Source: CSIS Economics Program.

In the smart city of tomorrow, fiber-optic networks, AI, and quantum will interconnect in digital infrastructure. Upgraded transportation networks, improved management of city utilities, and safer public spaces will depend on these systems, making their effective deployment critical to unlocking the **socioeconomic** benefits of smart city development. While key to the future of smart cities, each of the three constituent technologies discussed in this paper are only part of a broader technology ecosystem encompassing other IoT and network-enabling systems.

Meeting the Needs of Developing Economies

The stakes for expanding connectivity and smart city technology are immense and particularly acute in low- and middle-income countries (LMICs). According to the ITU, of the approximately **2.9 billion** people who do not have consistent access to the internet, **96 percent** live in the developing world. Rapid urbanization and population growth will intensify the demand for broadband and digital infrastructure. LMICs will host 17 of the world's **megacities** by 2030, heightening their participation in global networks. While many developed countries still lag in smart city deployment, the large and growth-oriented markets of developing economies will be a key theater for U.S.-China competition in this space. As Figure 5 illustrates, many present and future megacities located within LMICs participate in China's Belt and Road Initiative and have received technological exports from China. The United States and allies should provide realistic and attractive alternatives to meet the needs of developing economies in order to meaningfully compete with China.

Figure 5: Megacities of Tomorrow

Source: "Second International Conference on Water, Megacities and Global Change," UNESCO, https://en.unesco.org/events/eaumega2021/megacities.

Enhancing communications systems and digital infrastructure will be key to developing countries' participation in global networks and the broader digital economy. Urbanization will drive demand for smart city systems that improve traffic, public services, and safety. Expanding access to broadband will be the first hurdle in building urban capacity for smart city services. Dense urban environments will allow infrastructure investments to connect greater numbers of people and provide service providers with larger numbers of customers to support infrastructure expansion.

Fiber-optic cables can be used to connect emerging markets to the internet and help narrow the digital divide. As of 2021, the ITU estimates that 700,000 kilometers of underlying fiber-optic cables need to be built globally on top of existing broadband networks to close the digital divide. Access to 5G networks and quality and affordable broadband, both supported by fiber-optic networks, are necessary requirements for participation in digitized smart city services. Critically, where fiber optics would be most impactful is also where they are least present.

Deploying fiber optics in developing markets brings unique challenges. Lessons learned as the United States and other advanced economies continue to expand domestic fiber-optic networks will not always translate to other markets. While municipal governments are responsible for the rollout of fiber optics in the United States, this may not be the case in less-developed countries. Different starting points regarding digital infrastructure and different political structures create varying incentives, capabilities, and challenges. This point holds true for the implementation of smart city technology in cities across the world; there is great diversity in city governance, structures, and priorities even within a single country.

Energy, network maintenance, land rent, infrastructure security, and information availability can pose serious challenges to the deployment of fiber optics in developing and conflict-affected countries. The lack of up-to-date maps on where optical fibers are buried, for example, can be a costly challenge for developing countries looking to invest in smart city technology. One major source of optical fiber failures and mismanagement is the lack of accurate and available location data on network routes. Comprehensive and up-to-date maps or databases on fiber-optic networks can help identify areas of low fiber-optic density and areas where existing fiber optics are underutilized. The lack of an official communication channel between city officials, business leaders, and community developers makes it difficult for local governments to

effectively direct spending and infrastructure development. Cities also often run into roadblocks artificially created by federal guidelines that often do not have the granularity or flexibility to allow cities to respond to their unique challenges.

Planning for Competition

A UN report released in 2015 called for rejecting the view of smart cities as top-down end products to be provided by governments, instead favoring a layered approach to building services and improving transportation, connectivity, and land use. Unilaterally funded and planned smart cities built from scratch often result in failed or substandard outcomes, costing governments exorbitant amounts as projects drag on. Rwanda's plan for a "Vision City" is one telling example. Financed by Chinese firms in 2014, the proposed development of a smart neighborhood in Kigali was initially slated to cost $90 million. In a city where as much as 80 percent of the population lives in slums and makes less than $240 a month, the planned community aimed to build up to 4,500 housing units starting at $172,000. A few years later, with at least $36 million in cost overruns at last estimate, developers have had to slash prices over 60 percent to incentivize uptake on Vision City housing units and have fallen short of recuperating costs. Projects with similar scope and structure such as Toronto's Quayside neighborhood in Canada, Lavasa in India, and Masdar City in Abu Dhabi have cost governments far more than initially budgeted and have not delivered the benefits promised.

As noted in the 2015 UN report, promoting competition and choice for cities to develop organically is a better approach than directly planning for smart communities—smart cities need to be built atop of better functioning "dumb cities" to succeed. This involves addressing the underlying policy challenges that local governments need to tackle before resorting to complex technological solutions for bettering city services and infrastructure. Cultivating an environment that draws in competitive private financing to work in tandem with municipal-led finance, for example, is a policy challenge necessary for smart city development. Building transparent procurement processes that prevent elite capture and rent seeking is another.

There is a need to create capacity and technological know-how for local policymakers to ensure that the public's interests are being met when contracting with profit-oriented businesses and foreign governments. The high social and economic stakes of smart city technology, along with expensive costs to switch out underlying infrastructure, mean that the decision on who builds smart city infrastructure creates wide-ranging and lasting impacts. Public-private partnerships have a role to play in building smarter cities, but the rules of private involvement are less certain. Using fiber-optic and AI-enabled sensor data to generate ad revenue, for example, can be both a risk to privacy and an upside in creating funds to develop city infrastructure. Local policymakers need to be sufficiently prepared when entering contract negotiations with profit-minded firms to ensure that long-term public interests are being prioritized.

Creating competitive market conditions is not only important for ensuring efficient allocation of public resources but also for retaining maximum flexibility for cities moving forward. Ensuring interoperable and sustainable implementation of smart cities is critical for future expansion, especially as technologies continue to evolve. Chinese firms that provide "end-to-end" solutions, bundling large hard-infrastructure projects with services, are attractive to solution-seeking policymakers in the short term but prove problematic over time. The European Chamber of Commerce found that Chinese ICT standards often lack interoperability with non-Chinese companies and technology. Another study, drawing from interviews with municipal leaders across Africa, South Asia, and the United States, found that ICT technology built by Huawei rated low on interoperability and potential for integration with other services. China's position as the global financier of telecoms and smart city infrastructure, while preferable to no financing for developing markets, can run contrary to long-term host country interests.

Recommendations

As U.S. policymakers consider the global networks of 2030, they should define and promote a high-standard smart city model that scales promising technologies and balances the inputs of citizens, the government, and the private sector. Experience has shown that centralized planning is not a viable strategy for promoting the development of smart cities. Fostering competition and choice requires the United States to lead the digital domain by promoting policy and technical interoperability. The following recommendations are aimed at aligning U.S. and allied efforts to compete in tomorrow's digital infrastructure markets:

1. Leverage domestic investments. The most substantial action that U.S. policymakers can take to enhance American competitiveness over the next decade is to pass comprehensive legislation, such as the competitiveness bills currently working their way through Congress, that provides increased federal funding for R&D, particularly in technologies that can enhance municipal technological infrastructure and enable further innovation. Encouraging U.S. telecommunications operators to accelerate 5G R&D and deployment and adopt open-access policies, for example, would foster competition in the domestic 5G market and support exports to foreign markets. Aligning Department of Defense investments in future communications networks such as LEO satellite constellations with private sector efforts could also produce broader positive spillovers for quantum communications and the middle-mile and last-mile gaps in broadband delivery.

2. Step up capacity-building efforts. U.S. government engagement in third markets should emphasize cost-effective measures that help foreign decisionmakers navigate the complexity of adopting new digital infrastructure systems. One initiative would be creating shared platforms for fiber-optic mapping, allowing municipal governments to visualize the infrastructure that is already available and optimizing development efforts. Washington should also increase funding for capacity-building programs such as the Infrastructure Transaction and Assistance Network's Transaction Advisory Fund and expand access to this successful program to recipients outside of the Indo-Pacific region. Programs such as these will help developing countries manage contract negotiation, proposal evaluation, and the procurement process.

3. Coordinate U.S. and allied private companies. Expanding smart city technologies abroad is both a coordination problem—within and between countries—and a financial challenge. No single country or international institution can fulfill the global demand for investments in connectivity. Therefore, the Departments of State and Commerce should co-lead a new effort to establish public-private partnerships that catalyze financing to market and export smart cities technology. The U.S. International Development Finance Corporation (DFC) can elevate its support for digital connectivity projects that increase baseline capacity. This could be complemented by opening a new government office, as the European Commission has done, that lists certified smart city vendors and connects stakeholders across the developing world. These efforts should be coordinated with key allies through mechanisms such as the U.S.-E.U. Trade and Technology Council and the "Economic 2+2" process with Japan.

4. Align allied digital policy. Fragmentation of global norms on emerging technologies could harm both innovation and security of digital systems. Critical areas in need of consensus are national data privacy frameworks, lowering barriers to data flow, and aligning policies on technology transfer. To advance allied coordination on these issues, the United States should leverage initiatives such as the G7's Build Back Better World initiative, which includes digital infrastructure as one of its four areas of focus, and the Biden administration's proposed Indo-Pacific Economic Framework. Additionally, the United States should propose establishing a multilateral forum, potentially modeled on the Financial Stability Board, where like-minded countries can forge consensus around specific standards and regulatory approaches to digital infrastructure.

5. Lead standards-setting activity. Competitors to the United States have mounted ambitious strategies to assert digital leadership. The emerging technologies described in this report will require new frameworks built on comprehensive multistakeholder dialogue. The OECD's Blue Dot Network certification program should include a focus area on smart city infrastructure standards, supported by "Sustainable Smart City" bonds to fund high-impact projects. Domestically, properly resourcing NIST will allow the agency to fulfill its role as the U.S. representative on international standards-setting bodies (such as the ITU, International Organization for Standardization, and IEEE) and as a convener of key stakeholders, as well as to continue building on its promising AI Risk Management Framework. One priority is supporting common standards for regulating AI, defined as ensuring that high-risk AI systems are explainable to the end user and that all AI algorithms are rigorously tested for bias, transparently disclosed, and designed to provide end users a way to contact providers about concerns. ■

Matthew P. Goodman *is senior vice president for economics at the Center for Strategic and International Studies (CSIS) in Washington, D.C.* ***Akhil Thadani*** *is a program coordinator and research assistant with the CSIS Economics Program's Reconnecting Asia Project.* ***Matthew Wayland*** *is a research assistant with the Reconnecting Asia Project.*

The authors wish to thank the many experts and officials who attended the three roundtables associated with this project and provided helpful comments on drafts of this report. The analysis and views in this report are solely those of the authors.

This report was made possible through the generous support of the Japan Ministry of Internal Affairs and Communications.