2022-06

A MODERN GREAT WALL: PRC SMART CITIES AND THE A2/AD IMPLICATIONS FOR AFSOC

Bowman, John D.

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A MODERN GREAT WALL: PRC SMART CITIES AND THE A2/AD IMPLICATIONS FOR AFSOC

by

John D. Bowman

June 2022

Thesis Advisor: Thomas Jamison
Second Reader: Ryan Maness

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2022	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
A MODERN GREAT WALL: PRC SMART CITIES AND THE A2/AD IMPLICATIONS FOR AFSOC

5. FUNDING NUMBERS

6. AUTHOR(S) John D. Bowman

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

The People's Republic of China's (PRC) proliferation of smart cities—integrated, government-controlled urban surveillance networks—has increased the persistent stare of surveillance technologies globally. While the place of smart cities in strategic competition has been studied, the capability of PRC smart cities to achieve military ends like Anti-Access/Area-Denial (A2/AD) has yet to be explored by Air Force Special Operations Command (AFSOC). The structure and capabilities of PRC smart cities reveal potential A2/AD threats and exploitation opportunities for AFSOC. Using the Integrated Air Defense System (IADS) as a model, this study suggests that PRC smart cities can function as IADS-like weapon systems, with a dispersed network of surveillance technologies integrated via a centralized control layer. PRC smart cities could produce at least two A2/AD threats to AFSOC: denial of aircraft entry to airspace and suppression of logistics and sustainment requirements (e.g., electricity and fuel). Conversely, AFSOC can exploit PRC smart cities using cyber-attacks—such as distributed denial of service and software manipulation—to preserve access and placement. This thesis concludes that AFSOC should pursue two lines of effort by investing in both: "living off the grid" independent of smart city infrastructure and new cyber technologies and tactics for Suppression of Enemy Information Systems—actions to disturb smart city command and control—to combat and exploit PRC smart cities.

14. SUBJECT TERMS
smart cities, PRC, grey-zone competition, A2/AD, IADS, AFSOC, SOF, joint force, integrated deterrence, Integrated Air Defense System, IADS

15. NUMBER OF PAGES
97

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

A MODERN GREAT WALL: PRC SMART CITIES AND THE A2/AD IMPLICATIONS FOR AFSOC

John D. Bowman
Major, United States Air Force
BS, United States Air Force Academy, 2010
MA, Liberty University, 2017

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN DEFENSE ANALYSIS
(IRREGULAR WARFARE)**

from the

**NAVAL POSTGRADUATE SCHOOL
June 2022**

Approved by: Thomas Jamison
Advisor

Ryan Maness
Second Reader

Carter Malkasian
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The People's Republic of China's (PRC) proliferation of smart cities—integrated, government-controlled urban surveillance networks—has increased the persistent stare of surveillance technologies globally. While the place of smart cities in strategic competition has been studied, the capability of PRC smart cities to achieve military ends like Anti-Access/Area-Denial (A2/AD) has yet to be explored by Air Force Special Operations Command (AFSOC). The structure and capabilities of PRC smart cities reveal potential A2/AD threats and exploitation opportunities for AFSOC. Using the Integrated Air Defense System (IADS) as a model, this study suggests that PRC smart cities can function as IADS-like weapon systems, with a dispersed network of surveillance technologies integrated via a centralized control layer. PRC smart cities could produce at least two A2/AD threats to AFSOC: denial of aircraft entry to airspace and suppression of logistics and sustainment requirements (e.g., electricity and fuel). Conversely, AFSOC can exploit PRC smart cities using cyber-attacks—such as distributed denial of service and software manipulation—to preserve access and placement. This thesis concludes that AFSOC should pursue two lines of effort by investing in both: "living off the grid" independent of smart city infrastructure and new cyber technologies and tactics for Suppression of Enemy Information Systems—actions to disturb smart city command and control—to combat and exploit PRC smart cities.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

A2/AD	anti-access / area-denial
ACC	Air Combat Command
ACE	Agile Combat Employment
AFSOC	Air Force Special Operations Command
AI	artificial intelligence
BRI	Belt and Road Initiative
CCP	Chinese Communist Party
CFR	Council on Foreign Relations
COA	course of action
COTS	commercial off-the-shelf
CTAM	Contesting Theater Access and Maneuver
DDoS	distributed denial of service
DOD	Department of Defense
DSLAM	Degrading Sustainment, Logistics and Mobility
DSR	Digital Silk Road
eID	electronic identification
EMCON	emissions control
ETA	exploiting temporal advantage
FID	Foreign Internal Defense
GCC	geographic combatant command
GIS	geographic information systems
IADS	Integrated Air Defense System
IC3	integrated communication and control
ICT	information and communications technologies
IOC	Intelligent Operations Center
IoT	Internet of Things
ISR	Intelligence, Surveillance and Reconnaissance
JOC	Joint Operations Center
LIDAR	light detection and ranging
NPS	Naval Postgraduate School

NUP	New Urbanization Plan
OA	operating area
OPSEC	operational security
PLA	People’s Liberation Army
PRC	People’s Republic of China
SEAD	Suppression of Enemy Air Defense
SEIS	Suppression of Enemy Information Systems
SOCOM	Special Operations Command
SOE	state owned enterprise
SOF	special operations forces

EXECUTIVE SUMMARY

The People's Republic of China's (PRC's) proliferation of smart cities—integrated, government-controlled urban surveillance networks—are increasing the centralized control and persistent stare of the PRC's surveillance technologies globally. Though the place of smart cities in strategic competition has been examined by scholars, their relevance to Air Force Special Operations Command (AFSOC) as a form of anti-access/area-denial (A2/AD) remains unexplored. In light of new PRC doctrine to counter U.S. special operations forces (SOF) operations and AFSOC's preparation for gray-zone competition, this thesis uncovers the structure and capabilities of PRC smart cities to reveal potential A2/AD threats to and exploitation opportunities for AFSOC.

This research proposes that PRC smart cities can function as an IADS-like weapon system, with a distributed network of surveillance technologies integrated via a centralized control layer. Each of the IADS functions—surveillance, management, and action—is present in the PRC's smart city model. That model consists of three hierarchical layers—sensory, operations, and applications—that are centrally controlled. Furthermore, PRC smart cities ecosystem of technologies like internet of things (IoT), intelligent operations centers (IOC)s, digital twin, cameras, and light detection and ranging (LIDAR) give smart city operators the capability to monitor and control applications like smart grids and "safe cities"—cities that emphasize security. Many analysts have described smart cities as "ecosystems," but for AFSOC purposes, the IADS model has more utility.

Based on the IADS-like capabilities of PRC smart cities, this research distills potential threats to and exploitation opportunities for AFSOC, shown in Table 1. PRC smart cities could produce at least two A2/AD threats to AFSOC: increased risk or denial of aircraft entrance to airspace and suppression or denial of logistics and sustainment requirements (e.g., electricity, fuel, and internet). These threats come from PRC smart city applications like smart grids and "safe city" technologies and subsequently decrease OPSEC and covertness of aircraft and airman. Conversely, AFSOC can exploit PRC smart cities using cyber-attacks—such as distributed denial of service and software

manipulation—to preserve access and placement. Furthermore, it can exploit smart cities for information operations.

Table 1. Research Findings of Threats to and Opportunities for AFSOC

A2/AD Threats to AFSOC	Countering Access and Imposing Cost Opportunities
Increased Risk / Denial of Access for Movement and Maneuver: 1. Inhibiting aircraft access to airspace overtop smart cities for ISR, Fires and Mobility missions. 2. Decreased OPSEC for movement of personnel within the urban environments.	Suppression of Enemy Information Systems (SEIS): 1. Distributed Denial of Service (DDoS) attacks on vulnerable smart city infrastructure like IoT and IOCs. 2. Software hacking of- and malware placement in-digital twin for control of smart city applications.
Denial / Suppression of Logistics and Sustainment: 1. Preventing host nation supplies like water, gas, electricity, fuel, food, internet.	Detailed and sophisticated information operations to achieve an Information Advantage

This research concludes that AFSOC must pursue short- and long-term investments in preparation for its encounter with PRC smart cities. First, it must invest in its ability to "live off the grid." AFSOC must develop capabilities to reduce its reliance on host-nation technologies, and logistics and sustainment requirements. Second, it must develop new cyber technologies and tactics for Suppression of Enemy Information Systems (SEIS) to interrupt smart city command and control. Such actions include cyber-attacks against critical infrastructure like IoT devices and IOCs as well as digital twin software hacking. Though these recommendations are not all-inclusive, this research will help AFSOC avoid a strategic blind spot by preparing to maintain access and placement of personnel and aircraft despite PRC civilian technologies like smart cities.

ACKNOWLEDGMENTS

First, on a personal note, I want to thank my family, most importantly my wife, Adriana, and kids, for enduring this long but rewarding process. The move to California in the middle of a pandemic was not the easiest, but it was an experience we will all remember. I could not have done this without you all; thank you for the support.

On a professional note, I would like to thank Dr. Tommy Jamison and Dr. Ryan Maness for your incredible and indispensable support throughout the course of this thesis. Your leadership and mentorship were invaluable and something I will cherish. Thank you both for challenging me and making me a better officer.

Finally, but certainly not least, I want to thank Matt Norton at the Naval Postgraduate School Graduate Writing Center for his writing advice and for painstakingly guiding me through the editing process of this thesis. I really appreciate your patience. You have made me better writer. Thank you.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Smart cities are system of systems that integrate technologies in urban environments through the digitalization of almost everything. These cities integrate digital technologies that are capable of regulating and automating public services and can address problems like security, safety, and smart grid regulation. As such, smart cities have become an element of statecraft that the People's Republic of China (PRC) is openly tapping into as a soft power instrument for economic and political gain. Since the beginning of the COVID-19 pandemic, the PRC has drastically increased its investments in smart cities as part of its Belt and Road (BRI) and Digital Silk Road (DSR) initiatives.[1] In support of these efforts, PRC-based companies like Huawei are developing and proliferating smart city technology that will fundamentally change daily life in urban environments—spaces where nearly seventy percent of the world's population will live by 2050.[2]

The PRC's proliferation of smart cities as a soft power tool to achieve its economic and political goals has been frequently discussed in academic and policy circles. However, few have considered how civilian DSR technologies, notably smart cities, could achieve military ends like anti-access/area-denial (A2/AD)—a strategy to deny, degrade, or suppress access to a capability or domain.[3] In particular, the Air Force Special Operations Command's (AFSOC) Integrated Deterrence strategy reveals a strategic blind spot to how the PRC's DSR technologies (notably smart cities) might shape the operational environment; what this thesis refers to as the "military gap" in current accounts. Principally, smart cities digitalization of the urban environment results in omnipresence of surveillance technologies that, when integrated via highly centralized control, makes smart cities a weapon system for achieving A2/AD affects. Conversely, and of equal importance,

---

[1] Jonathan Hillman, "Disrupting China's Digital Silk Road" (presentation, National Defense University, March 31, 2021), https://nsiteam.com/disrupting-chinas-digital-silk-road/.

[2] Germaine R. Halegoua, *Smart Cities*, MIT Press Essential Knowledge Series (Cambridge, Massachusetts: MIT Press, 2020), 19.

[3] Joint Chiefs of Staff, *Joint Forcible Entry Operations*, JP 3-18 (Washington, DC: Joint Chiefs of Staff, 2017), I–15, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_18ch1.pdf.

PRC smart cities could also be exploited by AFSOC across multiple conflict domains to reduce risk to AFSOC aircraft and personnel seeking to gain access and placement.

In light of new PRC doctrine and strategy to counter U.S. special operations forces (SOF) operations, this thesis examines potential problems and opportunities that PRC smart cities could pose for AFSOC. It offers AFSOC new intelligence and planning considerations, recommendations for developing tactics, and future research requirements to ensure that AFSOC can access and place forces in the physical and digital urban environments of smart cities. In particular, it argues for further research and awareness of smart cities, and investments and tactics development to counter PRC smart cities through the Suppression of Enemy Information Systems (SEIS) and force protection measures to live "off the grid."

A. PURPOSE: PREPARATION OF THE SMART URBAN ENVIRONMENT

Given AFSOC's strategic shift to integrated deterrence and its need to access and place forces for grey-zone competition, this research explores PRC smart cities' potential A2/AD threats to and exploitation opportunities for AFSOC. The most recent AFSOC strategic guidance states the need to access and place forces despite our adversaries' A2/AD measures.[4] Successful modern A2/AD strategies seek to limit access and placement by reducing adversaries capabilities like movement and maneuver and sustainment and logistics.[5] Thus, all aspects of the PRC's unrestricted warfare, in all domains, must be analyzed from an A2/AD standpoint to ensure that AFSOC can access and place forces, regardless of an enemies military and non-military strategies. AFSOC's current or likely interaction with PRC smart cities in the future necessitates understanding the operational situation of PRC smart cities, which is an essential piece of this analysis.

---

[4] Air Force Special Operations Command, *AFSOC Strategic Guidance* (Hurlburt Field, FL: Air Force Special Operations Command, 2020), 10, https://media.defense.gov/2020/May/26/2002305551/-1/-1/1/AFSOC%20STRATEGIC%20GUIDANCE.PDF.

[5] Chris Dougherty, "Moving Beyond A2/AD," Center for New American Security, December 3, 2020, https://www.cnas.org/publications/commentary/moving-beyond-a2-ad.

B. RESEARCH QUESTIONS

Exploring the military implications of smart cities in the context of integrated deterrence, this thesis focuses on the A2/AD threats to and exploitation opportunities for AFSOC from PRC smart cities. It takes up five questions:

1. What technologies in PRC smart cities are of concern to AFSOC from an A2/AD perspective and what are their relevant trends both domestically and foreign?
2. Do smart city technologies integrate in a way that resembles other A2/AD methods, such as an Integrated Air Defense System (IADS)?
3. What threats do PRC smart cities pose to theater access and movement, and military mobility and logistics supply chains?
4. Do PRC smart cities present exploitation opportunities for AFSOC to increase access and placement and impose costs on the PRC?
5. How should AFSOC adapt to these potential realties?

C. METHODOLOGY / APPROACH

To answer the research questions, this thesis analyzes the A2/AD threats and opportunities presented by PRC smart cities using the concept of the IADS .The IADS is a model for conducting A2/AD in the air domain that integrates technologies to limit, deny, or increase the risk to an adversary—for example, a surveillance early warning radar tracking an aircraft and passing that data to a targeting or missile engagement radar. Structurally, the IADS is analogous to how smart cities integrate technologies and therefore provides a way of conceptualizing how different smart city technological components with different functions can be integrated to potentially achieve A2/AD. Qualitative data gathered from research on smart city companies and technologies and existing PRC smart cities forms the backbone of this research.

Within this framework, an operational thought experiment is used to describe AFSOC's potential interaction with PRC smart cities. This thought experiment is used to elucidate A2/AD threats to AFSOC's ability to access and place forces through joint

capabilities of movement and maneuver and logistics and sustainment. Additionally, it explores AFSOC's exploitation opportunities in the cyber and information domains, adapting principles of suppression of enemy air defenses (SEAD).

D. SCOPE AND LIMITATIONS

While this thesis uses the concept of the IADS to explore the A2/AD potential of PRC smart cities, the study does not make the case that smart cities *are* an IADS—though this topic is something for consideration by future researchers. Furthermore, this thesis does not speculate whether PRC smart cites are explicitly being built for A2/AD purposes. Finally, this thesis does not definitively conclude that the PRC will use smart cities in any military capacity. These remain vital topic of exploration but are outside of the scope of this work. This study only distills current information about PRC smart cities and identifies their *potential* use in A2/AD and the implications for AFSOC. That potential alone is reason enough, as will be shown below, for prudent investments.

E. CHAPTER OUTLINE

This thesis is organized into four chapters. Chapter II is a contextual overview, providing a definition of smart cities, a literature review identifying the problem and gap in understanding of the military implications of smart cities, and a theoretical framework of A2/AD and IADS. Chapter III analyzes the A2/AD potential of PRC smart cities. It establishes Huawei's Shenzhen's smart city as a pilot smart city and uncovers Huawei's smart city architecture. Further, it describes relevant technologies like Intelligent Operations Centers (IOC), cameras, and the Internet of Things (IoT) and then analyzes their ability to achieve IADS functions and tasks. Chapter IV applies that IADS structure of Huawei smart cities. Using an operational thought experiment, it identifies specific A2/AD threats to AFSOC from PRC smart cities. Additionally, it uncovers exploitation opportunities for ensuring access and placement of forces as well as imposing costs on the PRC. Lastly, Chapter V offers both short- and long-term recommendations for AFSOC to ensure it is prepared for its likely interaction with PRC smart cities.

II. SMART CITIES AND THE MILITARY GAP

PRC DSR cyber and smart city activities constitute a distributed network of surveillance technologies with significant political and strategic implications. Assessing what threats and exploitation opportunities smart cities might present to AFSOC personnel and aircraft from an A2/AD perspective requires three topics: first, explaining the origins of PRC smart cities, second, establishing the gap in literature regarding military A2/AD implications, and third, defining the A2/AD and IADS framework for analysis.

A. WHAT IS A SMART CITY?

Because no two smart cities are the same, experts have put forth a wide variety of definitions of a smart city to explain their purpose and utility. These differences can largely be explained by regional and ideological influences. Smart cities generally originate in three ways: as "smart from the start" cities with brand-new physical and digital infrastructure; "retrofitted cities" that digitally improve existing infrastructure; or "social cities" that use "sociality as an impetus for construction."[6] Their purposes likewise vary. Some smart city strategies seek to implement technologies to facilitate government services. Other smart cities utilize technology for functions such as security, environmental initiatives, smart health systems, and relieving traffic congestion, to name a few.[7]

The divergence in smart cities' purposes and origins stems from the regional and ideological—democratic vs. authoritarian—differences in how governments initiate and purport to use smart cities. Regional factors influence the ways in which a city becomes smart. For example, in Europe, smart cities are designed as "innovation hubs to strengthen

---

[6] Halegoua, *Smart Cities*, 65; Heather Andrus, "Creating the Smart City Through IOT-Based Retrofitting," *U.S. Tech Online*, 2017, http://www.us-tech.com/RelId/1764960/pagenum/2/ISvars/default/Creating_the_Smart_City_through_IoT_Based_Retrofitting.htm.

[7] Halegoua, *Smart Cities*, 25.

socio-economic progress."[8] In North America, smart city strategies focus on smart growth—"a collection of land use and development principles that aim to enhance our quality of life and preserve the natural environment."[9] Finally, in Asia, smart city strategies tend to focus on adopting advanced technologies to meet the land constraint and security issues arising from large populations.[10]

In addition to regional differences, political ideology plays a role in global smart cities, particularly the difference between top-down authoritarian governance and bottom-up government involvement. Democratic and authoritarian governments develop and use smart city technology in different ways. Democratic states, mostly in the West, have little central government involvement in smart city development. These cities start from a bottom-up approach, whereby "several actors independently" at the local level begin smart city projects.[11] By contrast, authoritarian states have a top-down approach to planning and beginning smart cities, as is the case in the PRC.

Reflecting its authoritarian political ideology, the PRC has followed a top-down approach to smart city development. Compared to democratic states, the PRC heavily directs the development of smart cities. Xi Jinping has made it a national priority to see smart cities developed to drive domestic innovation as part of the PRC's strategic economic modernization.[12] In April 2017, while visiting a smart city platform called the City Brain, Xi called on the PRC to make major cities "smarter by using big data, cloud computing

---

[8] Dong Lu et al., "The Performance of the Smart Cities in China—A Comparative Study by Means of Self-Organizing Maps and Social Networks Analysis," *Sustainability* 7, no. 6 (2015): 7605, http://dx.doi.org/10.3390/su7067604.

[9] Lu et al., 7605.

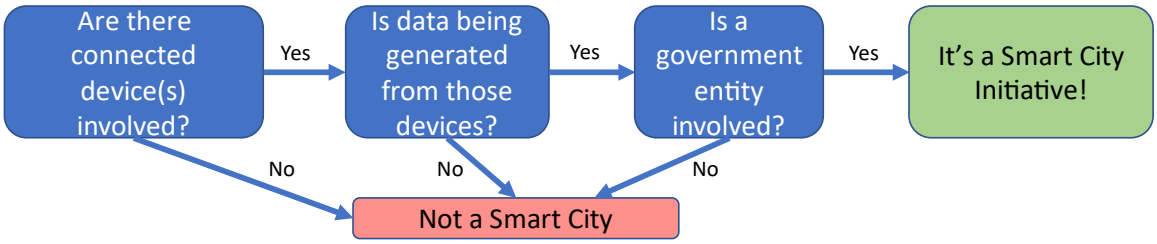
[10] Lu et al., 7606.

[11] Renata Paola Dameri and Camille Rosenthal-Sabroux, "Smart City and Value Creation," in *Smart City: How to Create Public and Economic Value with High Technology in Urban Space*, Progress in IS (Cham: Springer International Publishing, 2014), 2, https://doi.org/10.1007/978-3-319-06160-3_1.

[12] Xi Jinping, *Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era* (Beijing, China: Xinhua News, 2017), http://www.xinhuanet.com/english/download/Xi_Jinping's_report_at_19th_CPC_National_Congress.pdf; Richard Hu, "The State of Smart Cities in China: The Case of Shenzhen," *Energies* 12, no. 22 (January 2019): 7, https://doi.org/10.3390/en12224375.

and artificial intelligence technologies to modernize urban governance."[13] These national directives from the Chinese Communist Party (CCP) leader have led to government policies like the PRC's New Urbanization Plan (NUP). The NUP was set to run from 2014 to 2020, which called for promoting the construction of smart cities via a "new-generation of information technologies," among other things.[14] Xi and the rest of the CCP have since codified and prioritized developing smart cities broadly.

Despite their variety, there is one commonality among smart cities, including those of the PRC: the integration of technologies to form an ecosystem of sensors—along the lines of an IADS—that produces data for applications (see Figure 1). For example, a smart camera is limited in its capacity to address security problems. But integrated with other devices, technologies, and software, that camera can generate data for exploitation to produce an action.



This flow chart illustrates how to determine if a city is smart. Is there a distributed network of devices that forms a system of systems? If so, is some technology or mechanism filtering and exploiting its data? And finally, is a government entity involved to some degree? If all those criteria are met, then a city is a smart city.

Figure 1. What Is a Smart City?[15]

---

[13] "Xi Calls for Making Major Cities 'Smarter,'" *People's Daily Online*, April 1, 2020, http://en.people.cn/n3/2020/0401/c90000-9674926.html.

[14] "National New-Type Urbanization Plan (2014-2020)," Xinhua News, March 16, 2014, http://www.gov.cn/zhengce/2014-03/16/content_2640075.htm.

[15] Adapted from Chelsea Collier, "What a Smart City Is… and Is Not – Smart Cities Connect," Smart Cities Connect Media & Research, January 27, 2020, https://smartcitiesconnect.org/what-a-smart-city-is-and-is-not/.

Based on this commonality this thesis defines a smart city as a city that integrates information and communications technologies (ICT) into a "system of systems" for use in an urban area by government entities. These concepts are the foundation for the PRC's smart cities model, analyzed in Chapter III.

B. MILITARY SMART CITY GAP

Smart cities built and proliferated by the PRC exist in a larger context of the PRC's cyber capabilities and economic power. Literature commonly analyzes PRC smart cities through the lens of its cyber and economic advancement via its BRI and DSR projects. However, that same literature generally neglects possible A2/AD implications of PRC smart cities for the DOD or AFSOC.

1. PRC Cyber and Information Strategy

The PRC's strategic investment in cyber and information technologies and strategy are central components of its smart cities' surveillance technologies. The 2021 American intelligence threat assessment identified the PRC's cyber and information capabilities as advanced, leading the world in conducting surveillance and censorship globally.[16] The PRC views cyber and information as a natural extension of ensuring political and economic stability and uses them to influence populations and shape the operational environment in favor of the PRC's worldviews.[17]

Speculatively, the PRC's cyber and information policies and strategy are an outgrowth of its "three-warfares" strategy and material limitations vis-à-vis the United States.[18] The PRC's three-warfare strategy is a soft-power concept that uses asymmetric means—psychological, legal, and media warfare—to gain an advantage over

---

[16] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, Section 617 of P.L. 116–260 (Washington, DC: Director of National Intelligence, 2021), 8, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.

[17] Rogier Creemers, "National Cyberspace Security Strategy," *China Copyright and Media* (blog), December 27, 2016, https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/.

[18] Creemers.

adversaries.[19] Cyber, which certain PRC authors view its capabilities as an "assassin's mace," imbue the three warfare's with an asymmetric advantage.[20] What's more, this strategy is useful to the PRC because the PRC views itself as technologically inferior to the United States. Cyber has a low barrier to entry, enabling a more aggressive PRC cyber and information strategy.[21] However, vulnerabilities have developed in its aggressive strategy, and PRC authors have discussed its increasing weakness to cyber-attacks givens its offensive exposure.[22] Likewise, Kate Pisani analyzed PRC espionage via its social credit system and great firewall, which revealed PRC cyber vulnerabilities for exploitation by the DOD.[23]

Despite these vulnerabilities, in practice, the PRC uses offensive cyber and information to maintain CCP power by conducting espionage to steal foreign technology, coercing adversaries, and suppressing and controlling information domestically. Brandon Valeriano, Benjamin Jensen, and Ryan Maness argue that the PRC conducts more cyber espionage than any other country in the world because intellectual property and secrets are key to its growth and innovation.[24] In addition, while the coercive results are questionable, the PRC conducts espionage to coerce adversaries by leveraging the information stolen.[25] Finally, the PRC uses cyber in information warfare to suppress information and monitor citizens through technologies like the great firewall—security techniques to suppress

---

[19] Sangkuk Lee, "China's 'Three Warfares': Origins, Applications, and Organizations," *Journal of Strategic Studies* 37, no. 2 (February 23, 2014): 216, https://doi.org/10.1080/01402390.2013.870071.

[20] Simone Dossi, "On the Asymmetric Advantages of Cyberwarfare. Western Literature and the Chinese Journal Guofang Keji," *Journal of Strategic Studies* 43, no. 2 (February 23, 2020): 294–98, https://doi.org/10.1080/01402390.2019.1581613.

[21] Dossi, 294.

[22] Dossi, 301.

[23] Kate Pisani, "'Open Sesame': Identifying China's Cyberspace Vulnerabilities" (master's thesis, Monterey, CA; Naval Postgraduate School, 2019), https://calhoun.nps.edu/handle/10945/64048.

[24] Brandon Valeriano, Benjamin Jensen, and Ryan Maness, "China and the Technology Gap: Chinese Strategic Behavior in Cyberspace," in *Cyber Strategy: The Evolving Character of Power and Coercion*, Ryan (New York, N.Y., United States: Oxford University Press, 2019), 152.

[25] Valeriano, Jensen, and Maness, 143–70.

outside information—and social credit system—monitoring citizens' activities and information—to keep authoritarian tabs on and promote domestic stability.[26]

PRC smart cities are an outgrowth of its cyber technologies and strategies. That being, a means to enhance programs like its great firewall and social credit systems to preserve the CCP's power. Further, when this cyber and surveillance technology is coupled with economic programs like the BRI and DSR, it provides the PRC a mechanism for proliferating such technology globally.

2. Economic Development: BRI / DSR and Smart Cities

Coupled with its offensive cyber strategy, smart city development and proliferation are a facet of PRC economic development via its flagship projects: BRI and DSR. Economic components of foreign policy have played a central role in the PRC's ambitions for stability since the time of Mao. In *Haunted by Chaos,* the historian Sulmaan Khan asserts that the PRC's grand strategy since Mao has been a pragmatic and patient expansion of its economic capabilities domestically and globally in order to establish the PRC as a regional power, secure the state, and maintain lasting party power.[27] Khan sees the PRC's economic development and international assistance as fundamentally defensive. However, in 1999, two Chinese colonels, Qiao Liang and Wang Xiangsui, provocatively expanded economic and psychological measures for an offensive outlook, arguing for a whole-of-government approach to ensure the regional primacy and security of the PRC.[28] Whether the BRI and DSR are offensive or defensive is up for debate, but both are a part of a broader PRC strategy for economic development with critical military meaning.

---

[26] Pisani, "Open Sesame."

[27] Sulmaan Wasif Khan, *Haunted by Chaos: China's Grand Strategy from Mao Zedong to Xi Jinping* (Cambridge, MA; London, England: Harvard University Press, 2018).

[28] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Medina University Press International, 2021), loc 792 of 3643, Kindle.

a. Digital Silk Road

A key component of economic progress for the PRC is its DSR projects. The DSR—a subset of the BRI—is a central pillar in the PRC's economic expansion. Introduced in 2015, the DSR was created to assist the PRC's larger attempts to modernize its economy from a labor-based economy to one driven by technology innovation.[29] The DSR invests in and exports "digital technologies and business models" to facilitate the PRC's modernization of its economy in five areas: infrastructure, trade, finance, people's hearts, and policy (see Figure 2).[30]

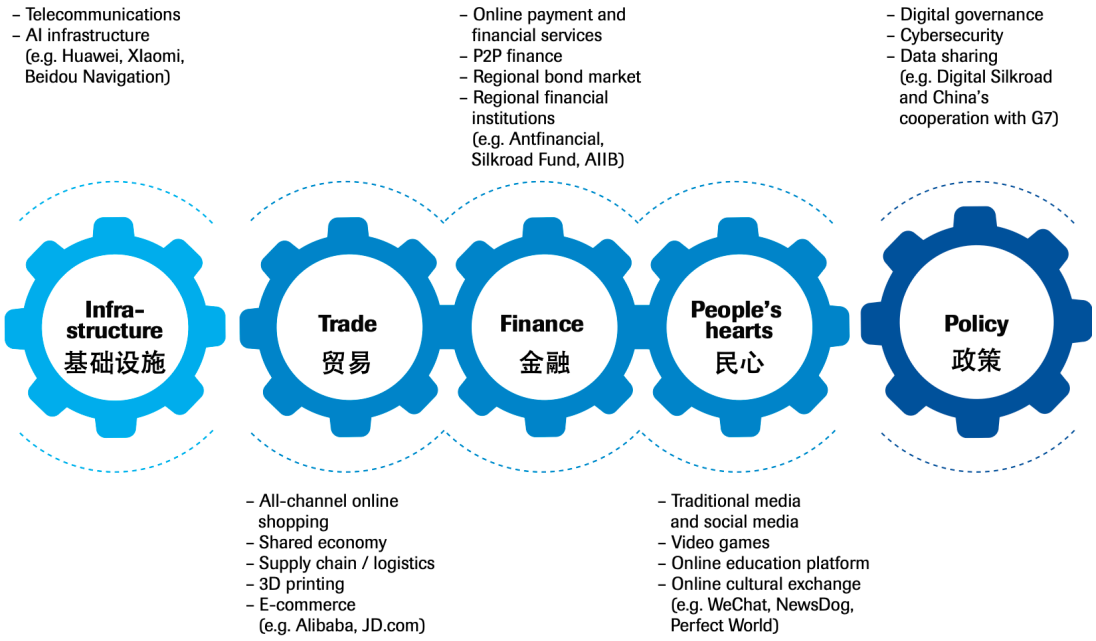


Figure 2. Components of the PRC's DSR.[31]

The DSR is currently little studied from an U.S. national security perspective. Jonathan Hillman asserts that the United States has been slow to comprehend the PRC's

---

[29] Brigitte Dekker, Maaike Okano-Heijmans, and Eric Siyi Zhang, *Unpacking China's Digital Silk Road* (Clingendael Institute, 2020), 3, https://www-jstor-org.libproxy.nps.edu/stable/resrep25693.

[30] Dekker, Okano-Heijmans, and Zhang, 4.

[31] Source: Dekker, Okano-Heijmans, and Zhang, 3. This figure was pulled by the authors from Fudon University Digital Belt and Road Center and translated into English.

digital expansion, particularly in Africa, and characterizes the DSR as the "most consequential" of its undertakings in the BRI given the PRC's ever-increasing market share in high-technology sectors and its consequent ability to set international digital standards.[32] As a consequence of the economic fallout from the COVID-19 pandemic, the PRC is aggressively marketing and selling digital infrastructure to middle-income economies since it is cheaper than more traditional BRI infrastructure projects and carries less risk politically and economically for the PRC.[33]

The proliferation of DSR digital technologies in middle-income economies aids in the PRC building an international surveillance network by pressuring states to conform to PRC's digital standards while also giving the PRC access to data and intelligence. The PRC is "moving from a being a rule-taker to a rule-maker on standardization" and "articulating" how it should be sold—a portion of its legal warfare strategy.[34] The Council on Foreign Relations (CFR) describes how the PRC sells complete technology packages, like smart cities, to cities and states, making it difficult and costly for those states to use "non-Chinese providers" after the purchase.[35] Thus, the PRC is creating a "China-centric technological order" that, via infrastructure like smart cities, gives the PRC potential access to intelligence and data that could be for military purposes.[36] However, those implications for AFSOC and A2/AD have not been addressed in the literature.

b. Smart Cities: More Than a Geopolitical Tool

While the literature describes the DSR as a soft-power tool, it stops short of articulating its implications for warfighters. That is, it does not explore the link between

---

[32] Jonathan Hillman, *The Emperor's New Road: China and the Project of the Century* (New Haven: Yale University Press, 2020), 174–75.

[33] Hillman, "Disrupting China's Digital Silk Road."

[34] Dekker, Okano-Heijmans, and Zhang, *Unpacking China's Digital Silk Road*, 10.

[35] Jennifer Hillman and David Sacks, *China's Belt and Road: Implications for the United States*, Independent Task Force, No. 79 (New York, NY: Council on Foreign Relations, 2021), 70, https://www.cfr.org/report/chinas-belt-and-road-implications-for-the-united-states/.

[36] Carolyn Bartholomew, "China and 5G," *Issues in Science and Technology* 36, no. 2 (Winter 2020): 51–52, http://www.proquest.com/docview/2452125915/abstract/CA8F81FEDAB413DPQ/1.

economic expansion, the civilian proliferation of cyber technologies, and their relevance to warfighters engaged in America's ongoing competition with the PRC. Literature on PRC smart cities is just beginning to emerge, but it recognizes smart cities as part of a Sino-American geostrategic battle and a means for the PRC to farm data and conduct espionage. While certain technologies that make up smart cities, like 5G, have been researched from a military perspective, scholars have yet to consider how smart cities integrate technologies in a way that has potential A2/AD implication for entities like AFSOC.

Some work explores smart city technology as a new instrument for the rapidly evolving strategic competition between the United States and the PRC. Alice Ekman's "China's Smart Cities: The New Geopolitical Battleground" establishes smart cities as the next Sino-American geopolitical competition, given that existing sectors of this competition, like 5G, make up the technological framework for smart cities.[37] More importantly, Ekman notes that Norinco—an equipment provider to the People's Liberation Army (PLA)—markets smart city products, further blurring the lines between their civilian and military use.[38] John Hemming's "Reconstructing Order: The Geopolitical Risks in China's Digital Silk Road" illuminates how smart ports, for example, might be used in a civilian context to slow the shipping traffic of certain states, which illustrates smart technologies being used as a geopolitical tool to disrupt markets or be a deniable "sanctions platform."[39] Still, the specific military ramifications of are unclear.

Much like the broader DSR, smart cities are also useful for data mining and espionage. A report prepared for the U.S.–China Economic Security Review Commission discusses many aspects of the PRC's smart cities development, most notably addressing the security threats from the PRC's capabilities to access global data and use it for PRC

---

[37] Alice Ekman, "China's Smart Cities: The New Geopolitical Battleground," *Etudes de L'Ifri*, December 2019, 7, https://www.ifri.org/sites/default/files/atoms/files/ekman_smart_cites_battleground_2019.pdf.

[38] Ekman, 10.

[39] John Hemmings, "Reconstructing Order: The Geopolitical Risks in China's Digital Silk Road," *Asia Policy* 15, no. 1 (January 2020): 19–20, http://www.proquest.com/docview/2355329399/abstract/E77E9684AC724836PQ/2.

intelligence agencies and development of its artificial intelligence.[40] Hemming echoes the challenges arising from the PRC's exploitation of data for economic and marketing advantage, which could impact America's geopolitical reach by hindering U.S. companies from entering those markets in the future.[41]

Not all aspects of the DSR and smart city have been ignored from an American military perspective. Former Naval Postgraduate School (NPS) students Mason Jones (a Navy officer) and Erica McCaslin (an Air Force officer) examine 5G technology—the backbone for smart cities—and argue that PRC 5G could force SOF to operate in high-risk telecommunications areas and threaten its ability to stay covert and minimize its signature management at the tactical level.[42] While Jones and McCaslin propose using deception measures to minimize signature management, their thesis implicitly assumes that entities like AFSOC can access and place forces in these high-risk environments. It should not be a foregone conclusion that AFSOC can access and place forces anywhere.

Overall, though current literature captures the PRC's cyber and economic expansion via the DSR and begins to establish the role of smart cities in the Sino-American geostrategic competition, a gap remains concerning the second- and third-order effects of PRC smart cities on AFSOC force projection—in particular, how PRC smart cities, with technologies like the IoT, digital twin, and facial recognition cameras, could participate in A2/AD.

C. THEORY OF A2/AD AND IADS

To fill the gap in knowledge regarding the A2/AD implications of PRC smart cities, requires first establishing what A2/AD is and how it suggests the model of an IADS—called the "kill chain." The IADS kill chain offers a way of conceptualizing adversaries'

---

[40] Katherine Atha et al., *China's Smart Cities Development*, Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission (Vienna, VA: SOS International, 2020), 80, https://www.uscc.gov/sites/default/files/2020-04/China_Smart_Cities_Development.pdf.

[41] Hemmings, "Reconstructing Order," 18.

[42] Mason P. Jones and Erica L. McCaslin, "Special Operations in a 5G World: Can We Still Hide in the Shadows?" (master's thesis, Monterey, CA; Naval Postgraduate School, 2020), https://calhoun.nps.edu/handle/10945/65560.

anti-access strengths and vulnerabilities by revealing fundamental nodes of integration of different technologies to achieve A2/AD—which is analogous to smart cities.

a. What is A2/AD?

In traditional military doctrine and strategy, A2/AD uses any means to prevent adversaries' access and freedom of maneuver in air, sea, and land domains. Joint Doctrine defines A2 as "those actions and capabilities, usually long-rage, designed to prevent an opposing force from entering an [operating area] (OA)."[43] It describes AD as "actions and capabilities, usually of shorter range, designed not to keep an opposing force out, but to limit its freedom of action within the OA."[44] However, doctrine implicitly emphasizes concepts of impenetrability, which does not fully describe PRC A2/AD activities.

In recent years, A2/AD has become more complicated because of the increasing prevalence of grey-zone competition and the evolution of warfare into new digitized domains—cyber and information. Chris Dougherty's modern A2/AD concept, exploiting temporal advantage (ETA), describes the PRC's A2/AD strategy as a manipulation of time by "either moving slowly or deniably to avoid provoking a response (e.g., Chinese island building in the South China Sea), or by moving quickly in areas where policies are unclear."[45] To do so, the PRC seeks information degradation and command and control disruption in all domains.[46] Because of adversaries new strategies in new domains, A2/AD is not only about holding or gaining a geographical space to complicate traditional domains but more broadly about disrupting an adversary's ability to achieve their own capabilities in all domains.[47] Thus, this thesis analyzes A2/AD capabilities of PRC smart cities as any actions or capabilities designed to increase the risk or cost to an opposing force of gaining access to a theater, domain, or achieving a joint function—A2—or to limit its freedom of action within a theater or domain in undertaking a joint capability—AD.

---

[43] Joint Chiefs of Staff, *Joint Forcible Entry Operations*, I–15.

[44] Joint Chiefs of Staff, I–15.

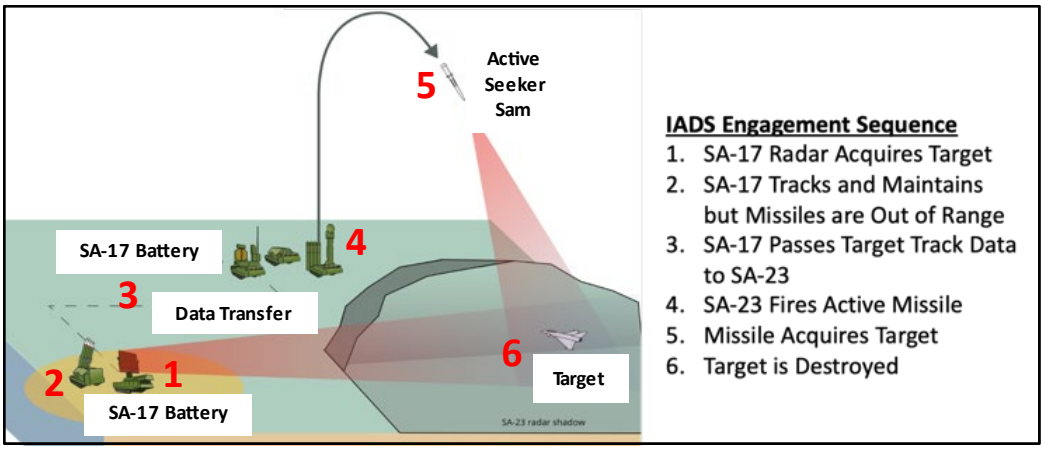
[45] Dougherty, "Moving Beyond A2/AD."

[46] Dougherty.

[47] Dougherty.

b. The IADS Model

The IADS, a manifestation of traditional A2/AD, is one method to pursue A2/AD in the air domain, and a useful model for discerning the A2/AD capabilities of PRC smart cities. The IADS integrates surveillance technologies with decision-making capabilities and weapons into a system of systems to counter an enemy's air assets tactically and strategically from penetrating territory to achieve capabilities like interdiction, air-to-air support, or other joint capabilities. The IADS is a deterrent mechanism that may not provide perfect protection but induces a high enough risk or cost that an adversary does not attack or attacks a target only once.[48] To achieve A2/AD in the air, an IADS accomplishes three core functions, integrated by communication technologies: surveillance, battle management and weapons control (Figure. 3).



This system of systems concept demonstrates an SA-17 surveillance radar, beyond its firing range, linked to an SA-23 to pass target information through some communication mechanism (e.g., satellite, data link, landline) for the SA-23 to fire a missile.[49]

Figure 3. Modern IADS Sequence.[50]

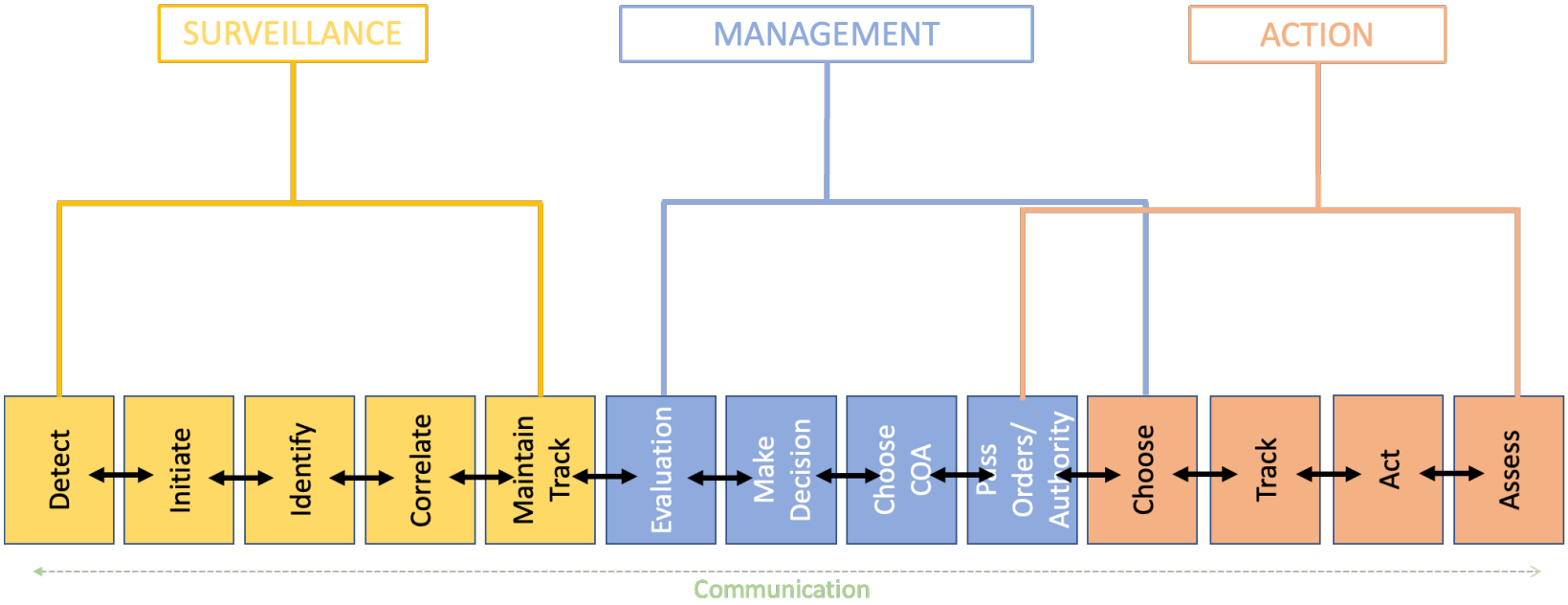
---

[48] Bryan F. Smith, "A Model of an Integrated Air Defense System (IADS) for the Tacops Program" (Thesis, Monterey, California. Naval Postgraduate School, 1991), 18, https://calhoun.nps.edu/handle/10945/26640.

[49] Justin Bronk, "Modern Russian and Chinese Integrated Air Defense Systems: The Nature of the Threat, Growth Trajectory and Western Options," *Royal United Services Institute*, January 15, 2020, 11, https://rusi.org/explore-our-research/publications/occasional-papers/modern-russian-and-chinese-integrated-air-defence-systems-nature-threat-growth-trajectory-and.

[50] Adapted from Bronk, 11.

While an IADS is a system of systems with functions for the air domain, this model is helpful in analyzing any system of systems, like PRC smart cities, that integrates technologies to determine their surveillance, management, and actionable capabilities to increase cost and risk for A2/AD purposes, including ETA, in any domain. For an IADS, we typically think of the output of the system being some kinetic effect (e.g., destroying an aircraft, drone, or low-observable missile); however, in other domains, there are other actions that would raise the risk and impose a cost on an adversary—for example, a police force could arrest a SOF team, or there could be an information campaign to influence populations against an adversary. Therefore, to avoid suggesting that the result of smart city A2/AD is purely "kinetic," this thesis refers to battle management as "management" and weapons control as "action." Figure 4 illustrates the adapted IADS model for this analysis.



The kill chain illustrates specific tasks of the IADS to achieve its functions of surveillance, management, and action. This depiction of the kill chain reveals fundamental nodes of integration for each of the functions. For example, in the management function, it must receive threat data from the surveillance function, evaluate the data, choose a course of action, and issue commands. Any interruption of this chain, at any one of the nodes—represented by the "black arrows"—could hinder the system's ability to produce an action.

Figure 4. The IADS Kill Chain: Functions and Tasks

This model assumes that, to the degree that any system is functionally surveilling, managing, and executing an action, it is raising risk or cost to an adversary seeking access to achieve joint capabilities and freedom of maneuver and therefore is achieving A2/AD to some degree. Hence, this model provides a mechanism for analyzing PRC smart cities' potential A2/AD capabilities and exploitation opportunities.

D. CONCLUSION

This chapter provided the concepts of what a smart city is, the military smart city gap, the A2/AD and IADS framework for analyzing PRC smart cities. The literature has established smart cities as a top priority for the PRC and a geopolitical tool in competition between the U.S. and PRC. As an extension of PRC cyber strategy and economic progress, smart cities proliferate significant surveillance and cyber technologies, the likes of which are insufficiently studied from an A2/AD perspective. Since an IADS is a system of systems using surveillance technology, they are useful for this analysis and bears the question of how similar they are to PRC smart cities. The following chapter uses the basic functions of the IADS model to uncover PRC smart cities architecture as a system of systems and to establish their potential military capabilities to achieve surveillance, management, and action against AFSOC.

THIS PAGE INTENTIONALLY LEFT BLANK

III. HUAWEI'S SMART CITY ECOSYSTEM

Though smart cities take many forms, in the PRC, Huawei (a PRC telecommunications company) smart cities conceptualization is basically consistent: that is a smart city model that integrates technologies hierarchically into a system of systems via a centralized platform. Huawei's centralized platform, called the "central nervous system" collects and fuses data into a common operating picture that gives local government entities, private companies, and potentially the PRC and PLA full situational awareness about activity in the urban environment. This model, coupled with its ecosystem of technologies (e.g., intelligent operation center (IOC), cameras, IoT, and digital twin), has IADS-like capabilities to control smart grids and "safe cities"—cities that emphasis security—which could be an A2/AD threat.

This chapter establishes Huawei's Shenzhen smart city model and its ecosystem, consisting of thousands of technology partners, as the archetype for PRC smart cities. Specifically, it uncovers the architecture of Huawei's model and then analyzes the potential for that model to achieve the core IADS A2/AD functions of the modified model. Next, to demonstrate the Huawei model in action, it introduces critical tools of Huawei's ecosystem before analyzing two examples of smart city applications: smart grids in the PRC and "safe city" in Nairobi, Kenya.

A. THE PILOT SMART CITY: SHENZHEN AND HUAWEI'S MODEL

Understanding Huawei's model and technological ecosystem requires first establishing it as the PRC's "pilot" smart city model. Huawei, which advertises itself as "leading the way in the integration of physical and digital worlds," is a PRC state-owned enterprise with close ties to the CCP.[51] In 2019, it had access to over $75 billion from the

[51] Huawei, "Smart City," Huawei Enterprise, accessed April 20, 2021,https://e.huawei.com/en/solutions/ industries/government/smart-city.

CCP in various forms, including loans, grants, and tax incentives.[52] Further, the CCP requires state officials to be present inside the company, with certain members having served in the PLA.[53] In addition, Huawei is compelled to "support, assist, and cooperate" with PLA intelligence services, with recent documents linking Huawei to broader PRC surveillance programs.[54] That close relationship has allowed Huawei to become a world leader in sales of 5G technology, gain an economic foothold in the ICT sector, and gain a competitive advantage for its proliferation of smart cities.[55] Huawei has quietly developed more smart cities than the European Union and U.S. and has taken its smart city projects global, with more than 160 Huawei smart cities in over 100 countries.[56]

Close government ties and the PRC's desire for top-down control of smart city development make Huawei smart cities broadly representative of all PRC smart cities. As Chapter II discussed, PRC President Xi has directed smart city implementation, and, reportedly, his central government ministries guide, monitor, and evaluate all smart city development.[57] The central government establishes pilot cities, then other PRC-created smart cities, domestic or foreign, tend to follow and in some cases imitate the development

---

[52] Chuin-Wei Yap, "State Support Helped Fuel Huawei's Global Rise," *The Wall Street Journal*, December 25, 2019, sec. Tech, https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.

[53] Lindsay Maizland and Andrew Chatzky, "Huawei: China's Controversial Tech Giant," Council on Foreign Relations, August 6, 2020, https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant.

[54] Eva Dou, "Huawei Documents Show Chinese Tech Giant's Involvement in Surveillance Programs," *The Washington Post*, December 14, 2021, https://www.washingtonpost.com/world/2021/12/14/huawei-surveillance-china/.

[55] Maizland and Chatzky, "Huawei."

[56] Hu, "The State of Smart Cities in China," 14.

[57] Wenxuan Yu and Chengwei Xu, "Developing Smart Cities in China: An Empirical Analysis," *International Journal of Public Administration in the Digital Age (IJPADA)* 5, no. 3 (2018): 77, https://doi.org/10.4018/IJPADA.2018070106.

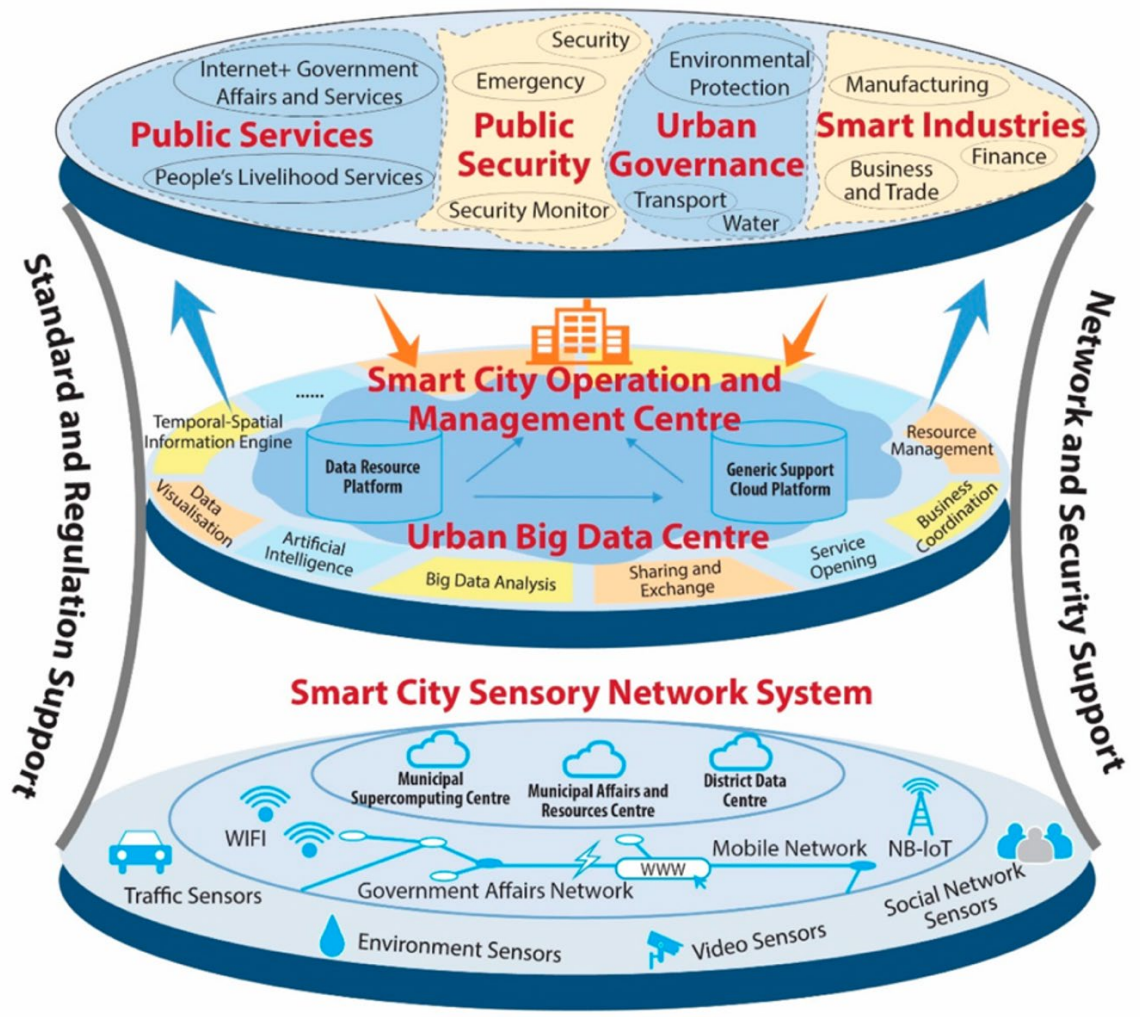
and structure of the pilot city.[58] Once such pilot city is Shenzhen smart city, which is ranked as the top smart city in the PRC and lead by Huawei's concepts and technologies.[59]

1. Huawei's Smart City Ecosystem: Centralized Control

Shenzhen's pilot smart city implements an architectural model for integrating technologies hierarchically via the "central nervous system"—the backbone of Huawei's smart cities. The Shenzhen model contains three layers—sensory, operation and management, and application—and achieves centralized command and control via the central layer. Figure 5 illustrates the smart city model in Shenzhen—the location of Huawei's headquarters.

[58] Lu et al., "The Performance of the Smart Cities in China," 7618. Example of foreign application: Shenzhen is working closely with Singapore through multiple agreements solidifying a smart city initiative.

[59] Hu, "The State of Smart Cities in China," 6.



PRC's Shenzhen smart city has three distinct layers. The lowest level of the technology hierarchy includes surveillance and data/information-collecting sensors. This layer feeds into the center layer, where IOCs, AI, and IoT collect, store, and disseminate data and make decisions for the third layer—the application layer—for applications like public security.

Figure 5. The Shenzhen Smart City Architecture.[60]

Though each layer in Figure 5 has separate functional outputs, the Huawei model emphasizes and achieves centralized control of operations by consolidating all the decision-making capabilities, knowledge, and operational picture in the middle layer. This capability is accomplished through what the company calls the "central nervous system."

[60] Source: Hu, 11. This diagram was originally sourced from the Shenzhen Government and translated into English. However, the original source was unavailable at time of writing.

According to Huawei, the central nervous system exerts unified control of technologies through artificial intelligence (AI), the IoT, and big data to "automatically collect and transmit" all city data.[61] In short, it funnels all knowledge, capabilities, and action through one layer of the smart city. While the central nervous system does not obviate the human element, its concepts are designed to make decisions autonomously and to automatically carry out applications. Taken from a Huawei smart city brochure, the significance of the central layer is illustrated in Figure 6, which shows the "central nervous system" at the top of the hierarchy and additionally demonstrates the model used in Shenzhen.

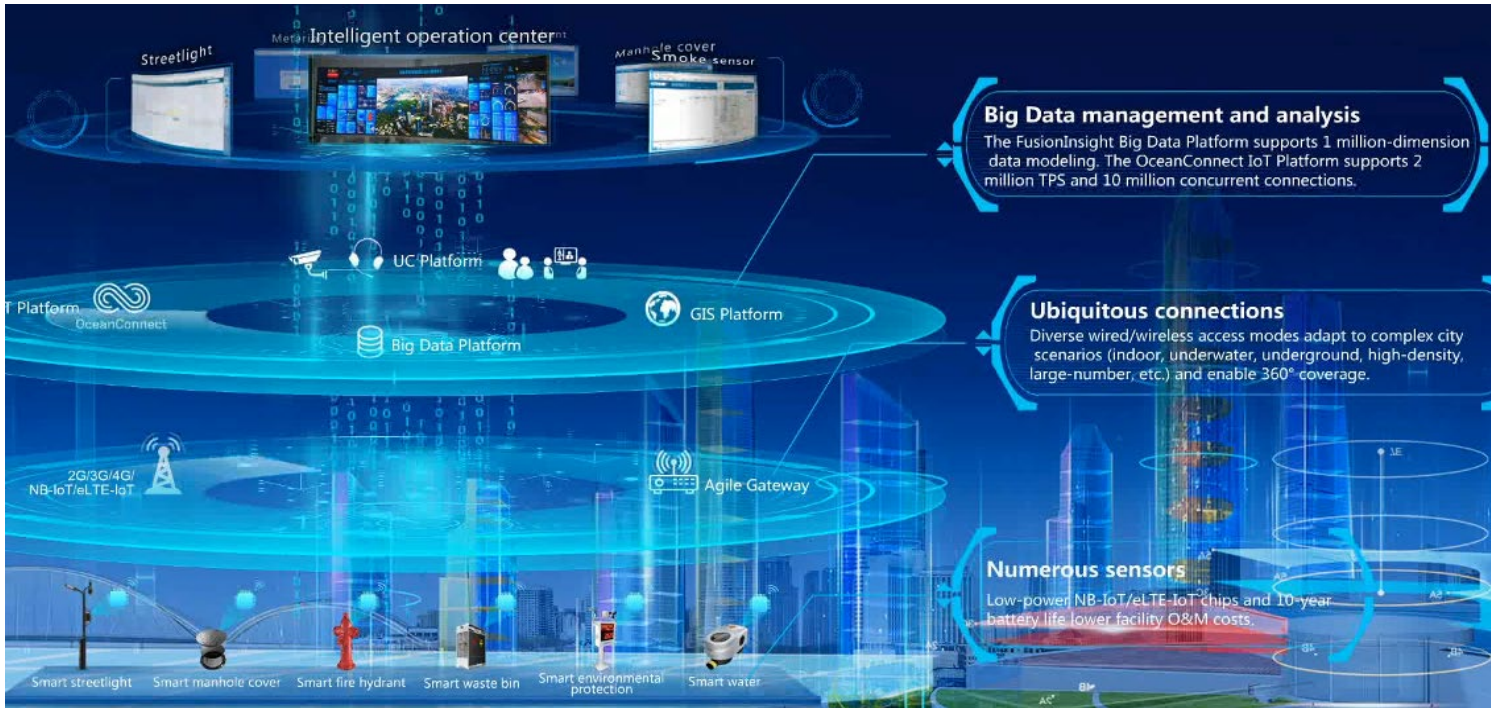
Furthermore, though this model is centrally controlled, it is also diversified and adaptable, allowing Huawei to create a PRC smart city ecosystem. The Shenzhen pilot smart city brings to light the hierarchical layers, and because Huawei smart city layers are "decoupled" (i.e., not dependent on each other), Huawei can quickly and efficiently add, remove, or switch technologies.[62] Generally, therefore, in this model, Huawei provides the architecture of the central nervous system, and its partners provide the sensors and applications. Huawei has a diverse set of thousands of technology partners around the globe, including American companies. For example, in Shenzhen, Huawei partnered with Honeywell to provide surveillance-enabled technologies like heating, ventilation, and air condition automation, which, via its open ecosystem concept, integrated Honeywell's technology into the central nervous system model.[63] This adaptability and diversification make PRC smart cities unpredictable, and it is this foundation which serves as Huawei's ecosystem, generating smart cities as a system of systems.

---

[61] Zhang Zhiwei, "Huawei Consolidates the Foundation of Smart Cities," *ICT Insights*, August 2018, https://e.huawei.com/en/publications/global/ict_insights/201806041630/special-report/201808170832.

[62] Huawei, *Building the Future: New ICT Enables Smart City* (Alexandria, VA: IDC Government Insights, 2017), 14, https://e.huawei.com/en/material/industry/smartcity/9b0000e57fa94a2dbc0e43f5817ca767.

[63] "Huawei Announces Collaboration with Honeywell to Develop Smart Building Offerings," Huawei, March 22, 2017, https://www.huawei.com/en/news/2017/3/Huawei-Honeywell-Smart-Building-Offerings.



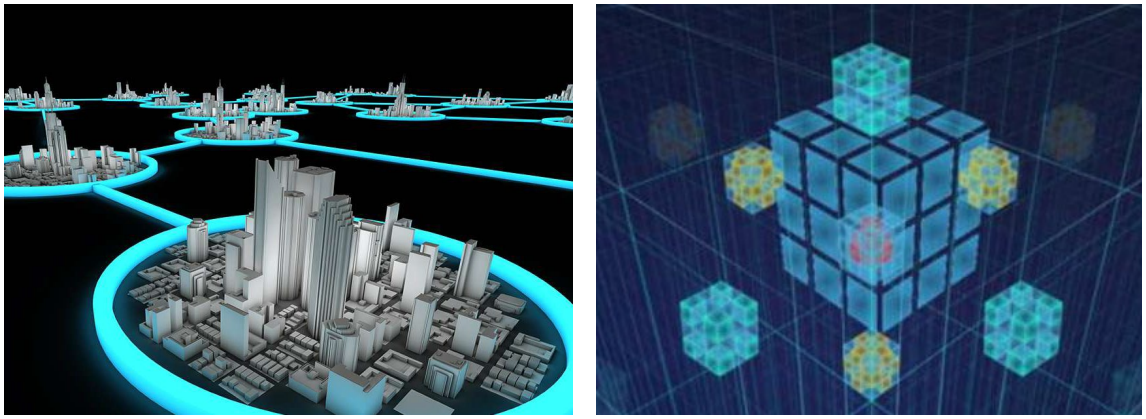
Taken from a Huawei smart city PowerPoint presentation, this depiction illustrates Huawei's smart city architecture with its emphasis on the central nervous system and management layer at the top of the hierarchy—further indication of the centralized control of PRC smart cities.

Figure 6. Huawei Smart City Brochure Advertising Hierarchy and Layers.[64]

64 Source: "Huawei Smart City Overview Presentation," Presentation, Huawei Enterprise, June 10, 2018, https://e.huawei.com/en/material/industry/smartcity/02ad4d5ab608492ea24659ec667f04bd.

2. The Cube: Integrating Smart Cities Globally

The centrally controlled PRC smart city model is further integrated by Huawei into a global network of smart cities. Huawei refers to its interconnected network of smart cities as the "cube" (see Figure 7). While at the local level Huawei's model is centrally controlled and adaptable, the cube concept provides Huawei, and potentially the PRC and PLA by proxy, centralized awareness and control of surveillance data at a regional or global scale.



The "cube" is a representation of Huawei's connected smart city network and illustrates its global adaptability and modularity. Each cube is itself interconnected to generate data and solutions for an individual city.[65] That individual cube is then connected to an ecosystem of global smart cities.

Figure 7. A "Cube" or Network of Global Smart Cities.[66]

Thus, the Shenzhen smart city is just one cube or "building block" in a global ecosystem that allows each smart city to operate independently but could create one common operating picture globally. This concept makes the PRC smart cities ecosystem more valuable than "the sum of its parts," as described by Edwin Diender, Huawei's chief digital transformation officer.[67] Therefore, Huawei advertises a potential future in which

---

[65] Edwin Diender, "Why One Connected City Is Not a Connected City," *Huawei BLOG* (blog), September 11, 2020, https://blog.huawei.com/2020/09/11/why-one-connected-city-not-connected-city/.

[66] Source: Diender.

[67] Diender.

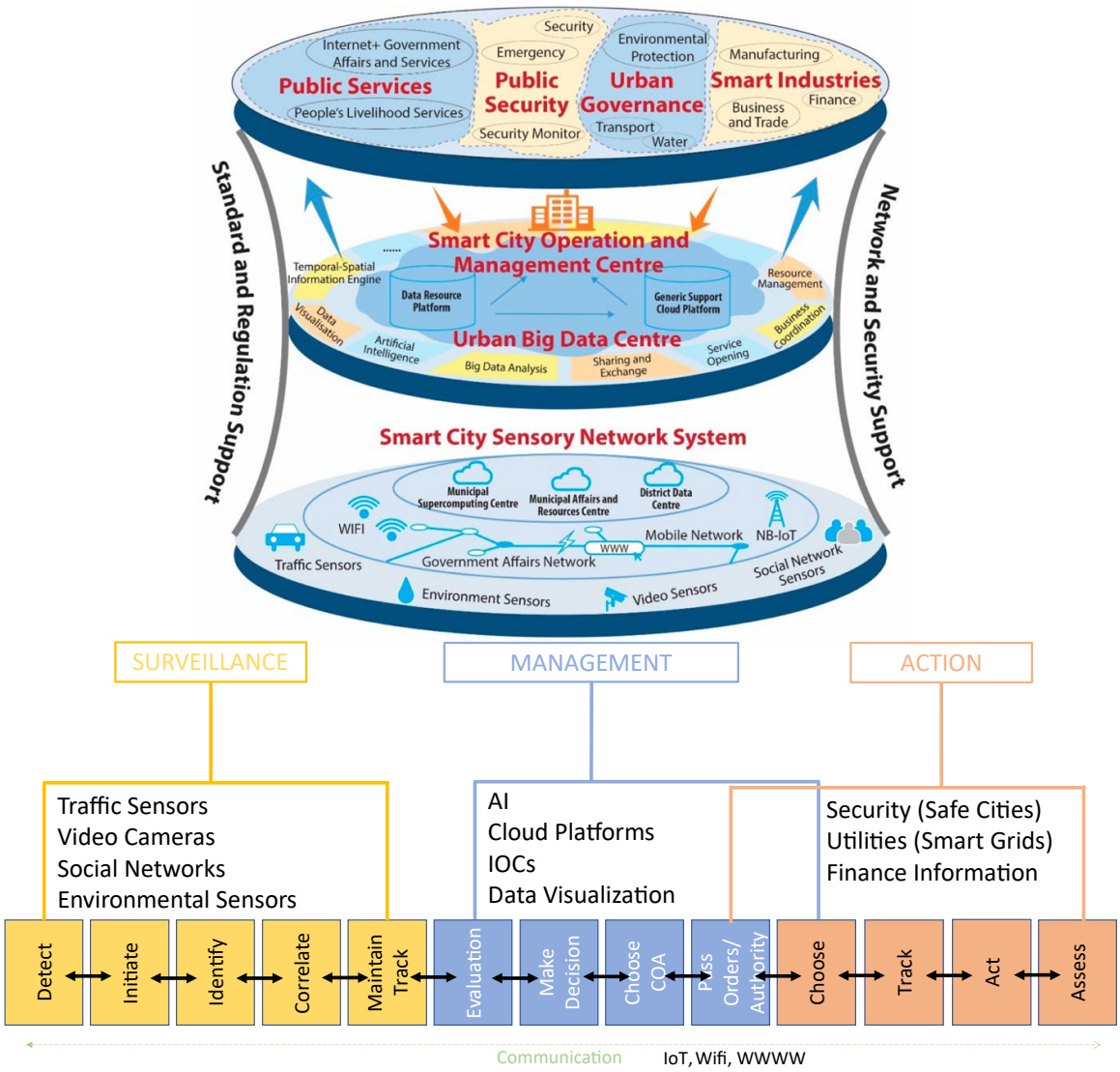
a facial recognition camera in Germany could digitally footprint an Air Force officer and that data could be instantly shared across all PRC smart cities and sent to the PRC and PLA for counter-intelligence exploitation. According to Diender, there are virtually no technical boundaries to implementing this sort of ecosystem.[68]

3. Shenzhen Case Analysis: Achieving the IADS Functions

Although the model for Huawei's smart cities seeks to achieve different outcomes, the model functions similarly to an IADS. Whether this resemblance is intentional or unintentional, the Shenzhen model is organized so that it surveils, manages, and produces action to some end.

Figure 8 places the concepts of the Shenzhen model alongside Chapter II's IADS kill chain. The bottom layer, the sensory network system, performs the surveillance function of an IADS. Traffic sensors, video sensors—for example, facial recognition—even supercomputing centers are all surveillance mechanisms in a city. This layer collects and logs the data to be passed to the central nervous system, labeled as Smart City Operation and Management Centre. This layer resembles the management function of the IADS by collating the information from the first function to exploit, fuse with other information, and make decisions. These tasks are done by big data centers, AI, business coordination, and managing resources available to the city. Finally, the top layer of the Shenzhen model resembles the action function of an IADS, whereby multiple applications are used to produce actions decided on in the second layer. Public security like emergency response teams, police and riot teams, and security monitors are examples of these types of applications in smart cities. Finally, communication technologies like WIFI, IoT, www, and mobile networks like 5G connect these three layers, much like in the IADS kill-chain model.

[68] Diender.



Illustrated here is the Shenzhen smart city model, with its layers, components, and technologies, placed into an A2/AD IADS kill chain model, which reveals a striking similarity between the Shenzhen hierarchical layers and the functions of an IADS. Each layer of Huawei's smart city model is designed to achieve the same functions as an IADS: surveillance (sensory level), management (operation and management centre), and action (application layer: public services and security).

Figure 8. Shenzhen Model as an IADS Kill Chain.[69]

69 Adapted from Hu, "The State of Smart Cities in China," 11.

At a more strategic level, like an IADS which can connect multiple sensors and weapon systems together, Huawei's cube concept creates an integrated network of surveillance tools. If Huawei interconnects these cities on a broader scale, they will functionally support each other to more broadly surveil and manage in a highly centralized fashion. Because the cube can collaborate and resource-share, the central nervous system can use data servers across multiple cities. Thus, Huawei claims the larger the system the faster and more efficient the system can be during large data surges.[70] The CCP's pursuit of centralized control through technologies that can be fully automated and linked to applications is realized in these smart city networks.

B. PRC SMART CITIES' TOOLS: TECHNOLOGY FOR CONTROL

Various technologies and tools enable the PRC smart city model in Shenzhen. Exploring a few of those technologies from the management and surveillance layers helps further reveal Huawei smart cities' IADS-like capabilities. Among the core technologies that the PRC's state-owned enterprises (SOE) are building include IOC, digital twin, and the IoT for management and cameras and light detection and ranging (LIDAR) for surveillance. This section offers a brief overview of each technologies' general capabilities in smart cities while also analyzing those technologies in the A2/AD IADS model, which reveals PRC smart cities' potential as an IADS-like weapon system.

1. Management: IOC, Digital Twin, and IoT

The foundation of Huawei smart cities' central nervous system is the management layer, or central nervous system. This layer is enabled by a combination of technologies like digital twin, AI, "big data," and the IoT that coordinate with the IOC to create

[70] Diender, "Why One Connected City Is Not a Connected City."

situational awareness and centrally control the smart city.[71] The combined capabilities of these and other technologies give the central nervous system the ability to achieve the core tasks of the management function of the IADS model.

a. IOC: Command and Control

In many Huawei smart cities, the IOC is the physical manifestation of situational awareness and control of the smart city. The IOC, commonly referred to by Huawei as the "brain" of the smart city, combines physical infrastructure and software to connect the numerous technologies in a smart city, producing a common operating picture and location for command and control.[72] Huawei advertises its operation centers as a "force multiplier" that integrates "a plethora of information sources" via its "large-screen displays, digital conferencing, sound reinforcement, video and audio switching," and centralized control systems (see Figure 9).[73] In addition to appearing strikingly similar to a joint operation center (JOC), IOCs fulfill roles similar to those of a JOC by being the primary command and decision-making center for the smart city.[74] In sum, the IOC provides Huawei and the PRC centralized control to make decisions and issue commands when needed.

---

[71] Smart cities use big data to provide data storage in quantities up to petabytes (PB), as well as data analysis. In addition, Smart cities use machine learning AI algorithms, to identify patterns and optimize usefulness to predict and implement the right decision for the smart city. "Smart City-Facilitating the Upgrade of City Infrastructure, Management, and Services," Huawei, accessed November 14, 2021, https://www.huaweicloud.com/intl/en-us/solution/smartcity.html; Vivek Kumar, "What AI and Machine Learning Can Do for a Smart City?," Analytics Insight, December 7, 2019, https://www.analyticsinsight.net/ai-machine-learning-can-smart-city/.

[72] "Huawei Creates a Smart City Nervous System for More Than 100 Cities with Leading New ICT," Huawei, November 14, 2017, https://www.huawei.com/en/news/2017/11/Huawei-Smart-City-Nervous-System-SCEWC2017.

[73] "Intelligent Operation Center Solution," Huawei, accessed November 1, 2021, https://e.huawei.com/en/solutions/industries/government/smart-city/ioc.

[74] Pei Yong, "Intelligent Operations Center: A Smart Brain for City Management," *ICT Insights*, November 2019, 37, https://e.huawei.com/en/publications/global/ict_insights/201908281022/focus/201911081641; Huawei, "Huawei Creates a Smart City Nervous System," 22.

Figure 9. Shenzhen IOC Command Center.[75]

b. Digital Twin: Algorithm of the City

Within the IOC and management layer is digital twin technology. A smart city digital twin is a computer mathematical model and digital representation of the physical smart city. As described by PRC scientists, the digital twin is a "simulation process" that uses the data from the physical world to represent the smart city in a virtual space.[76] The use of digital twin in the IOC allows city operators to conduct course of action (COA) analysis and predict outcomes based on surveillance-level inputs from Huawei's smart cities.[77] In other words, it manipulates computer algorithms to optimize the smart city. For example, the IOC could manipulate electricity outputs to different sectors of a city to see how it would affect energy consumption. Based on the model simulation, the digital twin can then directly implement the appropriate change for the smart city to conduct. In our example, the IOC could direct the digital twin to throttle electricity outputs based on how busy a sector of the city is to optimize energy resources.

---

[75] Source: "Leading New ICT, Building a Smart City Brain," Huawei, 12, accessed September 18, 2021, https://e.huawei.com/en/material/industry/smartcity/fd6fc58e324a4beba385fc00672e75a7.

[76] Li Deren, Yu Wenbo, and Shao Zhenfeng, "Smart City Based on Digital Twins," *Computational Urban Science* 1, no. 1 (March 29, 2021): 1, https://doi.org/10.1007/s43762-021-00005-y.

[77] Sue Weekes, "The Rise of Digital Twins in Smart Cities," Smart Cities World, January 6, 2019, https://www.smartcitiesworld.net/special-reports/special-reports/the-rise-of-digital-twins-in-smart-cities.

c. IoT: Communication and Connectivity

The IoT is the central mechanism for connecting millions of devices within the smart city management and surveillance layers to provide the IOC with situational awareness. The IoT is thus the interconnection of "physical and virtual things," which in smart cities links devices like smart cameras and IOCs so that they can communicate, interact, monitor, and share data across the city.[78]

To demonstrate the IoT's capabilities, consider this example: You are walking down the sidewalk and approaching a crosswalk. Embedded in the sidewalks are pressure sensors that sense foot traffic. A sensor detects movement, is connected to another sensor that calculates the gait, and passes that information to the traffic light to turn the signal red when you approach the crosswalk. The IoT makes that scenario possible. Without the IoT, smart city operators would not have situational awareness in the IOC or be able to control applications like smart grids, transportation systems, or city lighting, to name a few.[79] However, the IoT is highly susceptible to cyber hacking and as such, its strengths and vulnerabilities are intwined.

d. Management Technologies and IADS Tasks

The central nervous system's architecture and its technologies like IOCs, digital twin and the IoT allow it to achieve the management tasks in the IADS A2/AD model. From Chapter II, the management function of a system must evaluate something as a threat, decide, select the appropriate action, and issue commands or orders. The IOC has full situational awareness of the smart city and can evaluate threats and issues. It can make decisions automatically, via AI. Further, this layer can select the appropriate action using data analysis, via data centers, or human analysis, and it can issue commands and pair the appropriate authorities or teams to act. These capabilities make the IOC the centralized

---

[78] John Chen et al., *China's Internet of Things*, Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission (Vienna, VA: SOS International, 2018), 1, https://www.uscc.gov/sites/default/files/Research/SOSi_China's%20Internet%20of%20Things.pdf; Joe Appleton, "What Is IoT and Why Is It Important for Smart Cities?," *Bee Smart City* (blog), 2021, https://hub.beesmart.city/en/solutions/what-is-iot-and-why-is-it-important-for-smart-cities.

[79] Huawei, *Building the Future: New ICT Enables Smart City*, 21.

control for the smart city and give the PRC potential knowledge of and control over operations in cities, both foreign and domestic, like the management function of an IADS.

2. Surveillance: Cameras and LIDAR

Providing information to the management layer, the sensory level of Huawei's model taps into Huawei's partner ecosystem to use technologies like cameras and LIDAR for surveillance. It is in this layer that the CCP's authoritarian ideology manifests in vast surveillance capabilities, such as the existence of over 200 million domestic surveillance cameras in the PRC in 2018.[80] While certainly not all are part of smart city surveillance, the prevalence of technologies like facial recognition cameras and LIDAR allows smart cities to detect, and maintain track of people and objects for the IOC, thereby achieving the core tasks of the surveillance function of the IADS A2/AD model.

a. Cameras

The most well-known surveillance technologies in PRC smart cities are facial and vehicle recognition cameras. According to Huawei, its cameras are state-of-the-art, designed to be fully automated via AI, and can detect, identify, and track over 200 faces simultaneously, with 360-degree field-of-view awareness that can capture images in all weather and light conditions.[81] In addition to people, they claim to track 50 vehicles simultaneously and even identify the person driving the vehicle at up to 200 km/hr.[82] While impressive, the author could not find any data to support these camera statistic claims. This technology was most recently exposed by the *Washington Post* when it uncovered Huawei

---

[80] Atha et al., *China's Smart Cities Development*, 52–53. While in 2018 PRC had over 200 million cameras, the PRC had plans to increase that to around 626 million cameras by 2020, which equated to one camera for every 2.27 people in the PRC. Current estimates varied on the actual number as of 2021.

[81] Huawei cameras are software-defined cameras which give them the capability to use advanced algorithms to make existing "common cameras" more intelligent. "What Is a Software-Defined Camera?," Huawei, accessed November 14, 2021, https://e.huawei.com/en/products/intelligent-vision/cameras/software-defined-camera.

[82] Huawei's traffic surveillance cameras statistics claim a 95% effectiveness rate. "Huawei Vehicle Cameras," Huawei, accessed November 18, 2021, https://e.huawei.com/en/products/intelligent-vision/cameras/software-defined-camera/vehicle-micro-checkpoint; "Huawei Integrated ITS Cameras," Huawei, accessed November 18, 2021, https://e.huawei.com/en/products/intelligent-vision/cameras/software-defined-camera/electric-police-bayonet.

documents showing that its AI cameras can conduct behavior recognition by detecting sleeping workers (see Figure 10 on next page).[83] The report exhibits the breadth and capability of Huawei camera usage. This same technology is being developed for airports in Shenzhen, where passengers pass through security that includes facial recognition cameras and airport operators are using video cameras to supervise and track all aircraft activity on the airfield.[84]

b. LIDAR: Tracking Moving Objects

LIDAR is another sensor aiding PRC smart city surveillance. Using multiple laser beams to track objects, smart cities use LIDAR to track vehicles and even the direction and speed of pedestrians.[85] LIDAR enables automation in the smart city by creating an ecosystem in which all moving objects are tracked, tagged and collated with everything else in that area, including its surrounding.[86] Quanergy, an ICT company, is selling LIDAR capabilities in PRC smart cities like Hangzhou and Ningbo.[87] Though currently Quanergy LIDAR is being used on drones, in the future it could be expanded more broadly in smart cities for surveillance and tracking all activity, including drones, in the air around smart cities.[88] The significance for AFSOC could make it impossible for an aircraft to move or operate inside of a defined smart city if it is not communicating with the LIDAR technology.

---

[83] Dou, "Huawei Documents."

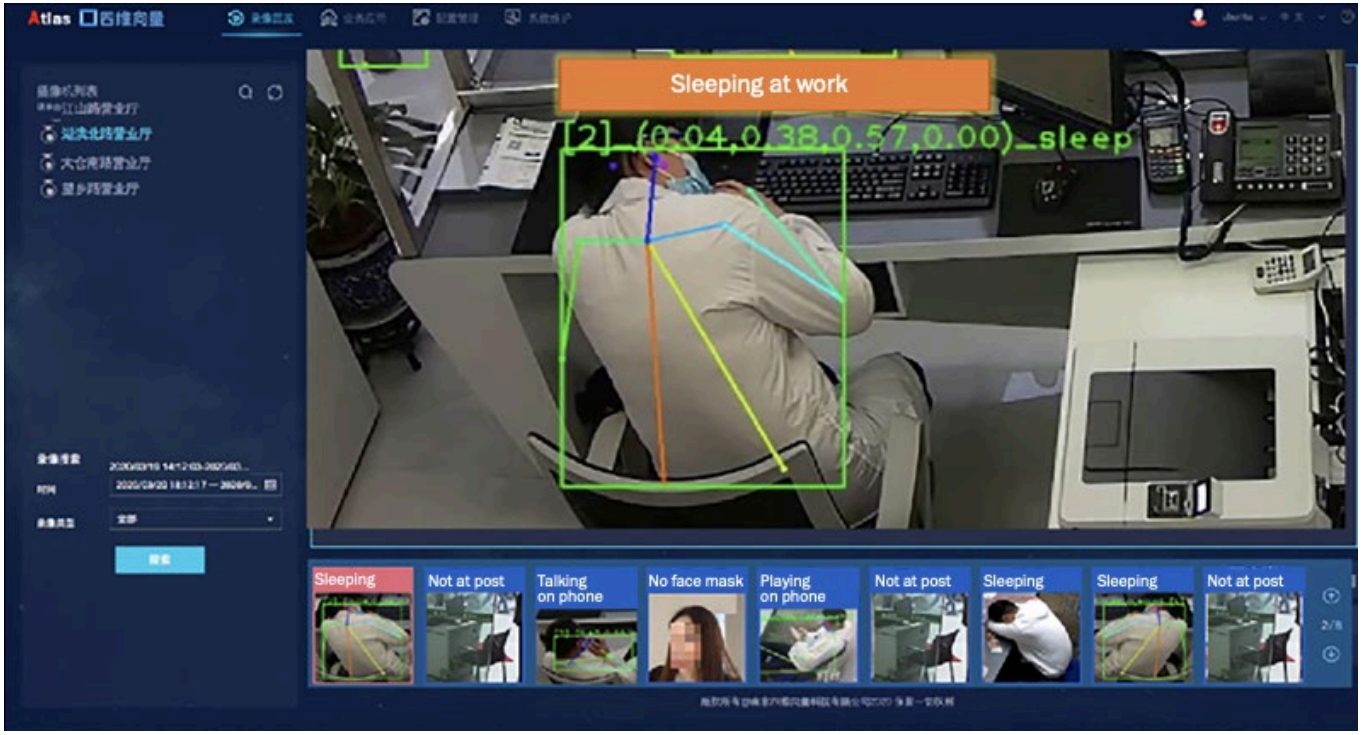
[84] Zhang Huai, "How Big Data and AI Will Transform Shenzhen Airport," Huawei, accessed December 15, 2021, https://www.huawei.com/en/technology-insights/publications/winwin/32/shenzhen-airport-digital-platform-and-ai.

[85] Adam Frost, "Lidar Sensors for Combined Smart City and Av Ecosystem," *Traffic Technology Today*, December 11, 2019, sec. Smart Cities, https://www.traffictechnologytoday.com/news/smart-cities/lidar-sensors-for-combined-smart-city-and-av-ecosystem.html.

[86] Frost.

[87] Frost.

[88] Frost.



The *Washington Post* uncovered this Huawei PowerPoint slide showing its AI cameras' ability to detect a worker sleeping. As the caption on the right reads, Huawei is advertising its cameras' capability to "identify people's actions and behaviors and send timely warnings through the system."[89] Such warning, for smart cities, could be going to supervisors, police, or the IOC for action.

Figure 10. Huawei Cameras in Action: Monitoring Human Behavior.[90]

[89] Dou, "Huawei Documents."

[90] Source: Dou.

c. Surveillance Technologies and IADS Tasks

The constant stare of PRC smart city surveillance technologies has the IADS-like capability to detect, identify, track people and objects, making this layer capable of achieving the surveillance function. Cameras and LIDAR can detect with high accuracy, initiate a track, and maintain custody—follow somebody or something. However, not all these technologies can identify or correlate. LIDAR, for example, cannot establish the identity of an individual. Other smart city sensors not discussed here, like sound and vibration detection, could detect and track to an extent but may not identify or differentiate with high accuracy. Nevertheless, in totality, Huawei smart cameras and associated technologies can detect, track, maintain, and identify, who, what, and where, which, combined with the IOC, is a powerful tool of the smart city that can achieve the IADS A2/AD function of surveillance.

C. APPLICATION OF HUAWEI'S MODEL: NAIROBI AND SMART GRIDS

The result of Huawei's smart city architecture and its technologies is applications. There are hundreds of smart city applications, including digital signage, kiosks, advertising, health and finance, environmental, security, government services, etc. However, two important applications best demonstrate the Huawei smart city model in action: safe cities and smart grids. Both applications show how the centralized control of smart cities produces an action, as in the IADS A2/AD model.

1. Huawei Safe Cities: Nairobi Case Study

Safe cities—an emphasis on security—display the Huawei smart city model in action. One safe city in particular, Nairobi, Kenya, highlighted the ability of the technology integration of PRC smart cities to catch a terrorist. In 2014, Nairobi signed an agreement with Safaricom in partnership with Huawei to install a smart city to address crime. Huawei's safe city project installed an impressive 1,800 cameras, 200 traffic surveillance cameras, and big data centers (for the full list, see Table 1). Most importantly, an IOC—called the integrated communication and control (IC3)—was installed to provide central control and awareness in Nairobi.

Table 1. Huawei's Safe City Exported Technology to Nairobi.[91]

Surveillance Technologies	Management Technologies	
1800 Cameras installed in Nairobi	Data Centers	2 el TE broadband trunking systems (allows for mobile relay of voice, video and data)
1500 HD Cameras	Video Cloud Node System of PB	GIS System
	2 TV Walls	New emergency Call Center
200 Surveillance Cameras	Unified Communications and Unified Video System	Analytics Software
	7600 el TE terminals to serve its 9000+ policemen and 195 police stations	

This table highlights Huawei safe city exported technologies to Nairobi that are sorted by their placement and usage in Huawei's smart city layers: surveillance and management.

Huawei's safe city in Nairobi was put to the test during a terrorist attack in January of 2019. It failed preventing Al-Shabaab terrorists setting off a bomb in a bank parking lot, along with a suicide bomb in the lobby of a hotel, killing in 14 individuals.[92] However, via its safe city infrastructure, once the attack was reported, the IC3 was able to quickly coordinate emergency response and track the terrorists. The IC3 and Nairobi police had instantaneous "panoramic video surveillance of Nairobi's urban center and a highly-agile command and dispatch setup" using satellites and geographic information systems (GIS) software.[93] The IC3 coordinated and communicated through its dispatch tracking network to find the nearest first responders and security teams and directed them to the site.[94] Simultaneously, the operators in the IC3 were able to analyze video footage—likely stored in the cloud or data centers—to "locate and retrace the attacker's vehicle" through the city's

[91] Adapted from Huawei, *Building the Future: New ICT Enables Smart City*, 29.

[92] "President Confirms Fatalities in Kenya Terror Attack," *Africa Times*, January 15, 2019, https://africatimes.com/2019/01/15/police-confirm-casualties-in-kenya-hotel-terror-attack/.

[93] "Safe Cities: Using Smart Tech for Public Security," BBC, accessed November 1, 2021, http://www.bbc.com/future/bespoke/specials/connected-world/government.html.

[94] N.D Francois, "Huawei's Surveillance Tech in Kenya: A Safe Bet?," *Africa Times*, December 17, 2019, https://africatimes.com/2019/12/18/huaweis-surveillance-tech-in-kenya-a-safe-bet/.

surveillance cameras, capable of license plate identification.[95] In less than 24 hours, according to *Africa Times*, the terrorists were apprehended, and the event was over.[96]

2. PRC Smart Grids and Digital Twin

Like safe cities, Huawei's smart grid applications demonstrate its smart city in action. Huawei is using smart city technology to monitor and control utility grids like electricity and water.[97] To do so, Huawei connects regular transmission lines, substations, water metering devices, and power plants to the IoT.[98] The integration of the IoT gives Huawei complete control of utilities, like gas line monitoring (see Figure 11). One example is in Shanghai, where Huawei has installed water metering devices connected to the IoT in residential buildings.[99] The devices monitor whether citizens' water usage is more than standard or not enough to suggest injury, and if the meters are triggered, local authorities are alerted to and dispatched for assistance.[100]

---

[95] "Kenya Fights Insecurity with Technology," The Kenya Alliance of Resident Associations, June 17, 2016, https://karakenya.wordpress.com/2016/06/17/kenya-fights-insecurity-with-technology/.

[96] Francois, "Huawei's Surveillance Tech in Kenya."

[97] Yan Lida, "Creating a Smart City 'Nervous System,'" *ICT Insights*, August 2018, https://e.huawei.com/en/publications/global/ict_insights/201806041630/commentary/201807131639.

[98] "Powering the Future with Smart Grids," Huawei, accessed April 13, 2022, https://www.huawei.com/en/technology-insights/publications/winwin/plus-intelligence/powering-the-future-smart-grids.

[99] "Building Happier Smart Cities," Huawei, accessed April 13, 2022, https://e.huawei.com/en/publications/global/ict_insights/ict31-digital-government/comment/smart-cities-that-provide-a-Sense-of-security.

[100] Huawei.

This image depicts an example of smart grid technology, in American, illuminating a smart meter, which is connected via the IoT, to transmit power usage rates to a central authority.[101]

Figure 11. Smart Meter for Public Gas Monitoring[102]

Furthermore, this technology is being integrated with digital twin in the central nervous system, to give city operators the ability to monitor, simulate, and inspect electrical grids. In total, the connection of smart grids to digital twin in the PRC extends to 15 provinces, including over 20,000 km of electrical line.[103] The smart grid integration with digital twin provides a virtual mapping of the electricity system to "reflect the entire life cycle process."[104] In other words, it can monitor in real time, determine faults, and report

[101] "Smart Cities," National Geographic, April 10, 2020, http://www.nationalgeographic.org/article/smart-cities/.

[102] Source: National Geographic, "Smart Cities."

[103] Deren, Wenbo, and Zhenfeng, "Smart City Based on Digital Twins," 6.

[104] Deren, Wenbo, and Zhenfeng, 5.

grid outputs, which, according to a PRC study, has been used in various situations like inspection of the grid during frost disasters, typhoons, and rain and fog (see Figure 12).[105]

Figure 12. PRC Smart Grid Monitoring during Emergencies[106]

Both the safe city and smart grid examples show how this technology architecture gives Huawei and the PRC government complete awareness and control of such applications. Specifically, both cases demonstrate the capability of Huawei smart cities to integrate surveillance data into the management level, like the IOC or digital twin, to produce an action. Furthermore, it exhibits the IADS-like capabilities of the PRC's hierarchical smart city model and ecosystem employed on both domestic and foreign soil.

D. CONCLUSION

Smart cities integrate technologies to utilizing information and making decisions to address challenges in the urban environment. For Huawei, Shenzhen's model displays a

[105] Deren, Wenbo, and Zhenfeng, 6.

[106] Source: Deren, Wenbo, and Zhenfeng, 7.

hierarchical structure that emphasizes strong centralized control through its central nervous system. Serving as the standard for PRC smart city architecture, Huawei's smart cities model and the technologies—IOCs, cameras, LIDAR, and the IoT—of its ecosystem reveal its capability of conducting IADS-like functions and tasks of surveillance, management, and producing an action. While Shenzhen is only one example, the model is being replicated throughout the PRC with smart grids and implemented globally in places like Nairobi.

PRC smart city technological integration clearly forms what most literature calls an ecosystem of surveillance technologies. *But*, from an AFSOC perspective, it is critical to consider this ecosystem as a potential IADS-like weapon system that is functionally designed to achieve surveillance, management, and action. Because the smart city can achieve IADS-like capabilities in a centralized and integrated fashion, it has the potential to achieve A2/AD. Chapter IV looks at those potential A2/AD threats and how the Huawei architecture for smart cities could be used to increase risk or impose a cost on AFSOC seeking to gain access or freedom of maneuver in grey-zone competition.

IV. AFSOC A2/AD IMPLICATIONS IN SMART CITIES

All AFSOC missions require the ability to access, place and sustain forces. To do so, AFSOC maintains freedom of maneuver with aircraft and personnel and supports such forces with logistics and sustainment requirements. But PRC A2/AD attempts to obstruct such capabilities. As discussed in Chapter III, PRC smart cities IADS-like structure and capability certainly pose A2/AD threats to and opportunities for AFSOC personnel and aircraft, but in what capacity?

To answer that question, this chapter first examines the nature of the threats posed to AFSOC. An operational vignette offers an illustration of the A2/AD threats AFSOC could encounter in the vicinity of PRC smart cities. Using this vignette, it analyzes how the IADS-like capabilities of PRC smart cities threaten AFSOC's ability to move and sustain forces. Secondly, the chapter explores AFSOC's ability to use cyber-enabled tools for access to reduce risk to aircraft and personnel and to gain an information advantage over the PRC. Overall, PRC smart cities IADS-like structure, and applications like smart grids and safe cities threaten AFSOC aircraft access to airspace, and ability to sustain forces with basic utilities. Nevertheless, AFSOC can use cyber-enabled tools like distributed denial of service (DDoS), digital twin hacking, and information campaigns, among others, to counter and impose cost on the PRC. Further, it suggests a need for AFSOC to "live off the grid," in order to reduce risk by relying on host-nation sustainment requirements.

A. A2/AD THREATS TO AFSOC BY PRC SMART CITIES

In grey-zone competition, AFSOC must be able to deploy and move forces into and throughout an OA to shape operational conditions and conduct its core missions like mobility, fires, ISR and all support functions.[107] To access and place forces, AFSOC seeks to attain the joint capability of movement and maneuver—the tactical and strategic positioning of forces *before* or *during* operations—and logistics and sustainment—the

[107] Joint Chiefs of Staff, *Joint Operations*, JP 3-0 (Washington, DC: Joint Chiefs of Staff, 2017), 37, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf.

coordination and provision of logistics and personnel services.[108] To achieve such capabilities, AFSOC relies on host nation, local government and even local armed groups to facilitate critical requirements like logistical supply chains, mobility, sustainment (e.g., fuel, food, water, internet), and operational security of physical areas within an OA.[109] The reliance on host nation support requires a degree of operational security (OPSEC) and covertness to ensure mission success. These operational principles are critical for AFSOC to access and place forces in the face of A2/AD.

Movement and maneuver and sustainment are threatened by modern A2/AD strategies that PRC smart cities posses with their IADS-like capabilities. As discussed in Chapter II, Chris Dougherty's ETA, breaks down modern PRC A2/AD into multiple strategies, two of which are contesting theater access and maneuver (CTAM) and degrading sustainment, logistics, and mobility (DSLAM).[110] Both CTAM and DSLAM A2/AD strategies are of great concern for AFSOC in conducting grey-zone competition. These strategies could increase AFSOC's risk to move and maneuver without the ability to access airspace in an OA and with degraded access to logistics and sustainment in support of those missions.

To illustrate the importance of movement and maneuver and sustainment in what could be typical AFSOC operations with respect to a PRC smart city, it will be helpful to provide a short operational vignette that makes clear the anti-access threats an AFSOC team may encounter while conducting operations. Though this vignette is hypothetical, it exists in a context of investments by the PRC in the Solomon Islands.[111]

---

[108] Joint Chiefs of Staff, 37, 47.

[109] Joint Staff Joint Force Development and Design Directorate (J-7), *Irregular Warfare Mission Analysis* (Washington, DC: Joint Chiefs of Staff, 2021), 39–40.

[110] Dougherty, "Moving Beyond A2/AD."

[111] See this news article for more information about the PRC's investments in the Solomon Islands. Low De Wei, "Why the Solomon Islands' China Pact Has U.S. Riled," Bloomberg, April 22, 2022, https://www.bloomberg.com/news/articles/2022-04-22/why-the-solomon-islands-china-pact-has-u-s-riled-quicktake.

Operation Bulldog Champs

Fifi is a geostrategic location for the United States for economic investment and military basing because of its proximity to PRC military bases in the region. The PRC has developed a relationship with Fifi, providing billions of dollars in aid. Most notably, Huawei has provided Fifi smart cities with surveillance systems like satellites, cameras, traffic cameras, LIDAR, IOCs, AI, and big data centers. Additionally, within the last year, Huawei installed smart airport technology and completed digital twin installations to monitor and run utilities, like fuel, and electricity.

Within the last 48 hours, hostilities between the United States and PRC have increased in the South China Sea, with close encounters between naval assets. Since the encounters, AFSOC aircraft (MC-130s, CV-22s, U-28s, and MQ-9s) and personnel in Fifi have been placed on elevated alert but tasked to continue supporting normal operations from Fifi to the rest of the geographic combatant command (GCC).

In the following hours and days, AFSOC personnel experience issues operating in Fifi not experienced before. As aircraft land in the regional airport of Fifi, unbeknownst to the pilots, airport cameras take pictures of the aircraft tail numbers and instantly uploaded to the IOC's database. As the aircrew deplane, facial recognition and tracking cameras on the tarmac take pictures and upload them for processing by Huawei's highly advanced AI algorithm for processing in the IOC. This information is processed and shared across the "cube" of smart cities back to the PRC. Now the PRC knows about United States military activity in Fifi.

Staying downtown in Fifi's capital city, AFSOC members drive to base the next day and see a local digital billboard proclaiming the occupation of Fifi by American SOF military. Further down the street, the crewmembers noticed a picture of one of their loadmasters on an emergency response bulletin alerting citizens to his "wanted" status by

capital police. Huawei traffic cameras are tracking the crewmembers' every move. AI recognized each individual and sent that information to the IOC, which was shared with the local PLA agents.

After conducting their mission while traveling back to the hotel, the crewmembers are again tracked and this time routed by the traffic management from the IOC using automated traffic lights and cameras in a completely different direction because of "construction" and light traffic issues. Unbeknownst to them, they are being sent into an area unsupportive of the American presence. Digital advertisement signage again begins to display profile pictures of team members with warnings in Fifi's native language of American military presence in the area and their potential for "nefarious" activity. Regional PRC agents and military members act on this information to alert the local Fifi police force to interdict the team members and question them about specific AFSOC members' activities.

Meanwhile, the base and aircraft are experiencing problems on the operational side. Most importantly, AFSOC aircraft like MQ-9s and U-28s were denied airspace because it did not have the proper communication transponders with smart city technologies like LIDAR. In one instance, the pilots pushed the situation to far, ignoring the denial of airspace, and were engaged by lasers in the vicinity of Fifi airports.

In addition, aircraft are unable to conduct resupply missions and fly ISR missions because the local airport is reporting "fuel shortages." Unbeknownst to American military personnel, Huawei digital twin technology monitors and controls local smart grids for fuel storage, electricity, water, and the internet. After becoming aware of American military presence, PRC officials modified the digital twin to shut off these resources at specific times. As a result, base infrastructure like electricity, water, and internet has "randomly" gone out for extended periods. In one instance, arriving at a remote field in Fifi, which has smart airport technology an MC-130's tail number is identified by AI smart cameras on

the tarmac, allowing airport operators to shut off fuel. In addition, logistics problems are mounting. The aerial port continues to report lost or undelivered items. Smart city technology has been diverting random cargo pieces by tracking their arrival and processing through pictures, AI, and the IOCs. The base is running low on supplies, and outposts cannot be resupplied as requested.

After one week, the situation in Fifi has deteriorated, and AFSOC's ability to conduct tactical missions is hampered; meanwhile the tensions between the PRC and the United States in the South China Sea increased even more. The GCC commander asks the commander in Fifi if they are ready to receive more troops as a possible deterrent against further PRC aggression. The commander reports back, "NO." They are unable to source reliable electricity, water, and internet for the base. Aircraft sortie success is degraded due to "fuel shortages, and airspace denial." He believes that the surveillance technologies and counter-intelligence mechanisms of Huawei's smart cities are being used in a centralized manner by the PLA to disrupt his team's ability to prepare the area for future assets. The commander recommends finding another location to stage future forces.

The Fifi vignette, again, while hypothetical, illustrates the IADS-like potential of PRC smart cities, with centralized management giving the PRC and PLA the potential to "weaponize" the surveillance data to produce A2/AD action against AFSOC forces. Specifically, the vignette exposes how smart cities' surveillance data and centralized control of that data produces two major threats to AFSOC's ability to access and place forces by PRC smart cities: degrading and denying access and maneuver through biometric tracking of persons and aircraft as well as disrupting, degrading, or denying AFSOC's logistics and sustainment requirements.

1. Degrading Logistics and Sustainment

The PRC IADS-like smart city is a vector for the A2/AD strategy of degrading logistics and sustainment. AFSOC's traditional reliance on host nation support for basing,

food, water, etc., make it particularly vulnerable to the suppression of these resources. The Fifi vignette suggested that PRC smart cities connected to smart grids, give the PRC and PLA an ability to deny these often taken-for-granted sustainment requirements in a battlespace.

A recent cyber-attack by the PRC in 2020 helps to illustrate the smart city A2/AD threat when connected to smart grids. In 2020, the PRC was engaged in a "border skirmish" with India. Months of engagement culminated in a cyberattack on Mumbai in October 2020 that shut down power to over 20 million citizens.[112] As reported by the *New York Times*, the PRC was behind the attack which forced the Indian government to shut down the Indian stock market; hospitals were forced to use backup generators during the peak of the COVID-19 outbreak, and all public transportation was halted.[113] While U.S. intelligence agencies have not publicly made full attribution, the cyberattack is a demonstration of PRC tactics against smart grids that could degrade logistics, sustainment, and mobility.

The Mumbai cyberattack was an attack on critical infrastructure not tied directly to smart cities, but it is an example of the type of threats smart cities pose to AFSOC. Through digital twin technology, described in Chapter III, and surveillance technologies like facial recognition technology and smart airports, the PRC now has the surgical capability to target AFSOC and other American military assets by controlling the smart grids AFSOC relies on. Smart cities provide the PRC with potential direct access to networks, electrical grids, and water supplies worldwide via their IOCs and the cube integration of smart cities. Instead of relying on malware placement, as was the case in Mumbai, the smart city itself is now "weaponized." Having knowledge of AFSOC team members and AFSOC aircraft provides the PRC the potential to use these smart cities as vectors for cyberattacks to shut down critical supply chains, internet, and electricity to AFSOC locations.

---

[112] David Sanger and Emily Schmall, "China Appears to Warn India: Push Too Hard and the Lights Could Go Out," *The New York Times*, September 27, 2021, https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html.

[113] Sanger and Schmall.

The PRC and PLA ability to use smart cities in this A2/AD fashion threaten AFSOC's access. The results of which mirrors an IADS threatening to shoot a military aircraft down, an increased risk or outright denial of accessing or operating in that OA. With this capability, aircraft could be grounded because of an inability to obtain fuel and planning cells might be interrupted with no connectivity or electricity. Further, supply chains for food, water, and critical supplies could be interrupted, directly impacting AFSOC's ability to conduct operations. The smart city thus reduces AFSOC's ability to rely on host nation support, which creates a new set of dilemmas for operating in austere, denied, and hostile environments during grey-zone competition.

2. Contesting Movement of Persons and Aircraft

In addition to a degradation in sustainment, PRC smart cities IADS-like weapon system threatens AFSOC's ability to access airspace with aircraft and move people. The Fifi vignette shows the potential for smart cities to give the PRC, PLA, and local authorities the ability to "weaponize" biometric and surveillance tracking to produce actions that denies or degrades movement and maneuver of AFSOC personnel and aircraft.

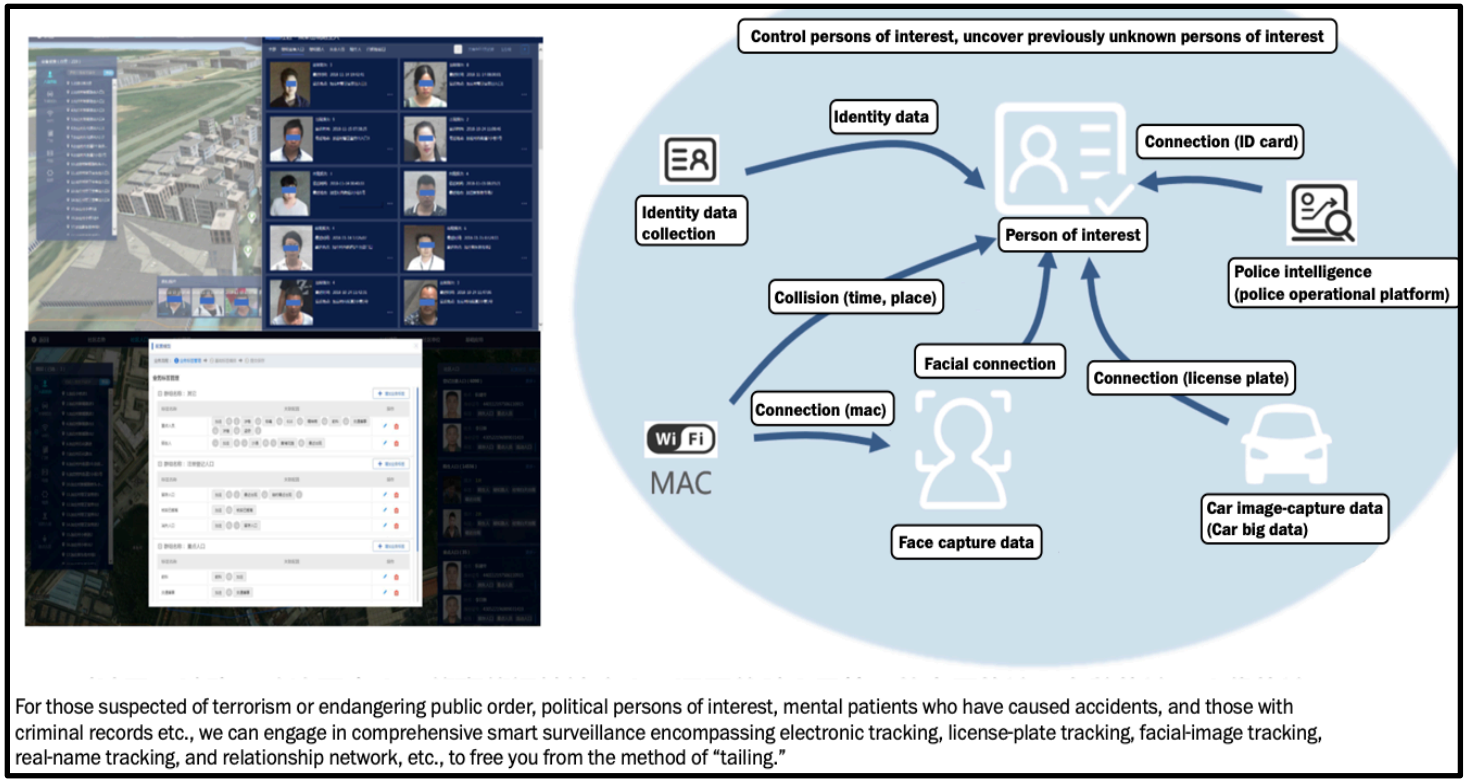
The tactic of tracking people and assets is not new to the PRC and PLA, and now the smart city is a potential "weapon system" to continue such activities against AFSOC. Reported by *The Washington Post,* it was discovered that Huawei has deliberately developed a network for tracking "persons of interests" for the PRC government and likely the PLA.[114] The report contained Huawei PowerPoint briefings to various PRC stakeholders showing the capability and value of a networked tracking system.[115] Figure 13 is an example of one of the slides from Huawei. It demonstrates Huawei's intent to support PRC requests for surveillance and tracking tactics with technologies that can capture faces, WiFi, and MAC address to track cell phones and vehicle data and correlate locations for police and security intervention.[116]

---

[114] Dou, "Huawei Documents."

[115] Dou.

[116] Dou.



This figure is Huawei briefing material advertising the capability to build a "smart profile" on a person of interest by collecting various data sources like cell phone data, facial pictures, and vehicle information. All this data collection is possible with smart city technologies.

Figure 13. Huawei Biometric Tracking Model.[117]

[117] Source: Dou.

While advertised as a tool to combat terrorists or interdict "person of interests," this model is easily applied against entities like AFSOC, via Huawei smart city technologies to contest the movement of persons and aircraft. First, the smart city technology described in Chapter III gives the PRC the capability to track AFSOC personnel through biometric analysis, degrading operational security and covertness, both threats to AFSOC operations. The IADS-like structure gives the PRC the unprecedented capability to centralize biometric and surveillance data to culminate in some sort of action. Those actions could vary from information operations, like displaying pictures and messages (as described in the Fifi vignette), to physical apprehension of personnel for detention and questioning. On top of those actions, there is a counterintelligence liability by giving away operational tempos and location of people and assets which increase risk to operate in such an environment.

This threat is not contained to one smart city or AFSOC operational battlespace. The cube connection of Huawei smart cities challenges the movement of AFSOC members on a global scale. The smart city can use facial recognition cameras, traffic cameras, and satellites in city centers, airports, and other locations to take pictures for processing and analysis in IOCs worldwide. To the degree that the PRC and PLA have access to every Huawei smart city throughout the globe, every AFSOC member identified is now in the PRC's database and could be recognized anywhere in the world. For example, an AFSOC member on vacation in Germany, identified as a military member during processing through Huawei smart airport technology, has a persona created and could be known in other countries on operational missions. This capability severely decreases attribution mitigation and covertness, essential to moving and maneuvering in grey-zone operations.

Secondly, all AFSOC aircraft could be denied access to airspace in the vicinity of or above smart cities. Specifically, the IADS-like structure of Huawei smart cities described in Chapter III, could potentially enable smart cities to be the vector for drone identification and tracking tactics. In 2018, Huawei teamed up with Unifly to use 5G technology to "follow drones in real-time, but also to determine who is flying, where they

are flying and whether they are permitted to be in that airspace."[118] This technology combined with LIDAR, digital twin and other smart city applications could be expanded to all types of aircraft to provide general defense and detection.[119]

The combination of Huawei and Unifly's technology with smart city technologies like LIDAR, cameras and satellites creates an ecosystem that could put AFSOC aircraft at risk of losing access to airspace, as well as covertness and attribution. If AFSOC aircraft do not have Huawei-specific equipment to communicate with smart cities or drone identification systems, they risk airspace denial or worse in the case of MQ-9s, exposure to anti-drone technology that could lethally take out AFSOC aircraft. The specific results could prevent AFSOC's ability to conduct airdrop resupply, ISR and close air support missions. Most critical, ISR assets like U-28s and MQ-9s ability to collect intelligence overhead urban areas could impacted. This denial of airspace and reduced intelligence capacity would severely cripple AFSOC's ability to move and maneuver. All told, the effects of Smart Cities could severely reduce the capabilities of AFSOC and ultimately increase the risk for AFOSC to access and place forces where needed.

B. SEIS: AN OPPORTUNITY TO EXPLOIT SMART CITIES

The advancement of smart cities by the PRC threatens to compromise the operational reach and capability of AFSOC aircraft and personnel. However, we should not be discouraged by this outlook. Instead, as Major Dan Meegan noted of digital infrastructure, AFSOC should look for opportunities in the same digital terrain to exploit PRC smart cities to AFSOC's advantage.[120] Much like the counter to IADS, SEAD, there

---

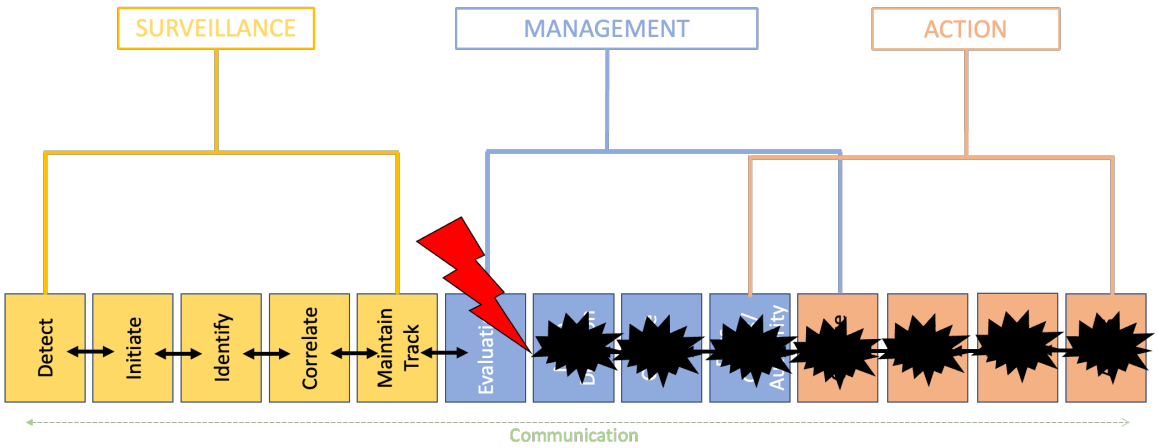
118 "Huawei and Unifly to Work Together on Drone ID and Tracking UTM Integration," UAS Traffic Management News, June 11, 2018, https://www.unmannedairspace.info/uncategorized/huawei-unifly-work-together-drone-id-tracking-utm-integration/.

119 James Blackman, "China Unicom, Huawei Test 5G 'Super Sensing' for Drones, Transport, Digital Twins," Enterprise IoT Insights, December 17, 2021, https://enterpriseiotinsights.com/20211217/channels/news/china-unicom-huawei-combine-on-5g-super-sensing-for-drone-detection-road-transport.

120 Major Meegan's thesis suggest that technologies can be both an asset and carry their own vulnerabilities, which in the case of smart cities is an increased connectivity. Daniel Meegan, "Breaking Other People's Toys: Sabotage in a Multipolar World" (master's thesis, Monterey, CA; Naval Postgraduate School, 2020), https://calhoun.nps.edu/handle/10945/66686.

are opportunities for AFSOC to create new and similar tactics like what this thesis calls, Suppression of Enemy Information Systems (SEIS), to counter PRC smart cities for access and exploitation of the information environment. The results could give AFSOC intelligence and geographical access to urban areas occupied by PRC smart cities.

Before delving into countering smart cities' A2/AD, a note on SEAD is needed to understand the potential tactic of SEIS. Air Force Doctrine defines SEAD as the "activity to neutralize, destroy or degrade enemy surface-based air defenses by destructive or disruptive means."[121] To do so, combat Air Force target key nodes or "chains" in the IADS to degrade the system of systems for exploitation in the air domain. A way to conceptualize SEAD is to refer to the IADS kill chain presented in Chapter II: and by removing or degrading a link in the chain, the total system can be neutralized, destroyed, or degraded for a period or permanently (see Figure 14). This concept provides a period of advantage for operations.



The lightning bolt represents an action to remove the management level's ability to evaluate the data from the surveillance layer, authenticate it and then make a decision. Such action has a downstream effect on the chain's ability to accomplish the rest of the tasks.

Figure 14. Targeting a Kill-Chain's Nodes

[121] Department of the Air Force, *Counterair Operations*, AFDP 3–01 (Maxwell AFB, Montgomery, AL: Air University, 2019), https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-01/3-01-AFDP-D02-AIR-Counterair-Operations.pdf.

In theory, SEIS can apply the same principles and concepts in the information environment to cyber and digital systems like smart cities to gain access and placement of AFSOC aircraft and personnel. The concept of SEIS was first considered in Dr. John Arquilla's work on information dominance in a 1994 article in *Strategic Review* called "The Strategic Implications of Information Dominance." He argued for a systems approach, targeting enemies' center of gravity to gain information dominance.[122] He defined information dominance as "knowing everything about an adversary while keeping the adversary from knowing much about oneself."[123] Thus, like SEAD, SEIS can gain an information advantage for a period, by targeting key information nodes of the smart city kill-chain. SEIS tactics are a potentially viable concept against PRC smart cities because of their vulnerability at the surveillance and management layers. To illustrate this vulnerability, it is instructive to provide a case example of PRC smart city failure as the impetus for this discussion.

1. Zhengzhou: PRC Smart City Failure

In July 2021, the city of Zhengzhou (population 10 million) experienced torrential rainfall, with 66 citizens reportedly killed during the rainstorms and subsequent flooding.[124] Zhengzhou recently had smart city flood sensors and software installed by the Zhengzhou Smart System Technology Company that was supposed to "monitor water levels in real-time through sensors and 'intelligent analysis' and notify relevant departments of incoming dangers."[125] However, citizens were not warned of the flooding, and the city did not take appropriate actions.[126] The inaction by the city, due to a multitude of factors at the surveillance and/or management level (e.g., faulty sensors, network

---

[122] John Arquilla, "The Strategic Implication of Information Dominance," *Strategic Review*, 1994, 24–30, http://hdl.handle.net/10945/41668.

[123] Arquilla, 25.

[124] Che Pan and Masha Borak, "Did Zhengzhou's Much-Hyped Smart City Projects Fail to Prevent the Floods?," *South China Morning Post*, July 28, 2021, sec. Big Tech, https://www.scmp.com/tech/big-tech/article/3142898/china-floods-smart-city-system-capabilities-called-question-after.

[125] Pan and Borak.

[126] Pan and Borak.

failures, poor calibration or the local city operators not acting) led to nationwide criticism in the PRC.

This example demonstrates weaknesses in smart cities that could be exploited. By disrupting the surveillance or management layer of Huawei's smart city model and associated technologies, AFSOC can at a minimum cause enough confusion for city operators, PRC officials, or PLA intelligence to not see or trust the data coming from the smart city. The possible areas of attack include conducting DDoS attacks on IoT devices and IOCs, hacking digital twin models to control smart grids, and using smart city technology to conduct influence operations to gain an information advantage over the PRC. Combined tactically, each of these tools could contribute to SEIS, a new way of countering information systems like smart cities.

2. DDoS Attacks at Surveillance and Management Layer

One method to interrupt the smart cities "kill chain," or command and control, is conducting DDoS—cyber enabled operation that overwhelms a computer or network, rendering it unusable for a short period—attacks to disrupt the surveillance and management layers by exploiting significant IoT vulnerabilities. The PRC has a long history of IoT devices being inherently insecure. For example, in 2017, more than 175,000 IoT cameras built by Shenzhen Electronics were hacked.[127] In 2016, the Mirai botnet infiltrated Hikvision and Zhejian cameras and IoT devices to launch DDoS attacks.[128] Additionally, PRC companies like Huawei leave backdoors on many of their devices, making remote access easy.[129]

Given that the IoT is one of the communication and management backbones for PRC smart cities, the neglect by PRC companies to robustly secure the IoT devices provides AFSOC an avenue into the surveillance and management layers to facilitate

---

[127] Chen et al., *China's Internet of Things*, 10.

[128] Chen et al., 10–11; Corinne Reichert, "US Finds Huawei Has Backdoor Access to Mobile Networks Globally, Report Says," CNET, accessed March 10, 2022, https://www.cnet.com/tech/mobile/us-finds-huawei-has-backdoor-access-to-mobile-networks-globally-report-says/.

[129] Reichert, "US Finds Huawei Has Backdoor Access."

placement of its aircraft and personnel into airports and urban areas under smart city surveillance. Useful areas of attack include Huawei surveillance, facial recognition, and traffic cameras, as well as Huawei IOCs. Using Shodan—a search engine that can scour the internet to identify insecure IoT devices—AFSOC planners can identify weak IoT devices in PRC smart cities. For example, a cursory search for Huawei and Hikvision cameras yielded over 4 million cameras worldwide, further pinpointing them down to the country, with over 300,000 in China alone.

Using Shodan to discover insecure IoT devices, AFSOC can infiltrate those systems to gain access to the IOC and launch simple sabotage attacks like DDoS "phlashing." Phlashing is a faster and cheaper form of DDoS where the cyber attacker gains access to weak network hardware and remove firmware, rendering the entire system unusable.[130] Through SEIS, as in SEAD, AFSOC can time phlashing DDoS attacks on cameras and IOCs that are timed with either landing at an airport or moving throughout the city for an objective. For example, if timed with aircraft arrival at an airport, it would allow AFSOC to land and offload cargo, and people without facial recognition or smart airport technology cataloging the event and uploading to the IOC for PRC exploitation. More broadly, if needed, the DDoS could be scaled to the entire city to disrupt Huawei 5G networks and internet access, thus bringing the city to a theoretical digital standstill. Applying this sort of tactic to Fifi, AFSOC crews could have timed phlashing attacks on sectors of their route, rendering the IOC unable to monitor the cameras in the first place. The result is no communication and decision making from the PRC. In total, the surgical targeting of smart city in this way could facilitate AFSOCs access and placement.

3. Manipulate Digital Twins and Smart Grids

Along the same line of effort, AFSOC can disrupt and degrade the management layer of the smart city by directly manipulating the digital twin or place malware in facial

---

[130] Neeta Sharma, Mahtab Alam, and Mayank Singh, "Denial of Service: Techniques of Attacks and Mitigation," *Journal of Computer Science Engineering and Software Testing* 1, no. 2 (July 1, 2015): 3, https://www.researchgate.net/profile/Neeta-Sharma-7/publication/296561817_Denial_of_Service_Techniques_of_Attacks_and_Mitigation/links/56d6987908aebabdb400c5d9/Denial-of-Service-Techniques-of-Attacks-and-Mitigation.pdf.

recognition, thereby confusing human operators and AI algorithms in the IOC. For example, AFSOC, partnered with Cyber Command, can use cyber tools to hack the digital twin models of PRC smart cities. With enough planning, the digital twin models code could potentially be modified, or AI algorithms changed to produce a new model for the smart city that is advantageous to AFSOC. SEIS tactics, like SEAD, can time the execution of this option, with movements into and throughout the city or airport, in addition to ensuring smart grids operate and provide sustainment requirements when needed.

Using the Fifi vignette as an example, manipulating digital twin code or placing malware in facial recognition code, prior to the AFSOC crewmembers' movement in the urban environment could have forced cameras into looking at a different location or deceived the recognition process. Another possibility via digital twin is interfering with 5G communication to hinder drone and aircraft identification when employing aircraft overhead the city for ISR. The disruption could disable the communication system for drone identification. Finally, for more sustained operations, the digital twin could be manipulated and continuously so, for the base of operations, at the airport, to receive electricity at specific times of the day or aircraft fuel to ensure the operational tempos could be met with some predictability. These actions reduce the risk to AFSOC aircraft and personnel and degrade the smart cities' capability to have a complete operational picture of AFSOC activities in the urban environment. In the same fashion as SEAD, this concept could be implemented into SEIS, for an information dominated period, to target specific nodes of the smart city for whatever effects are needed by AFSOC personnel and aircraft.

4. Gaining Information Advantage

What's more, while not directly related to access and placement, manipulating digital twin codes, conducting DDoS attacks, and sabotaging the application layer gives AFSOC and the joint force an informational warfare capability to influence populations. First, using tactics described above, AFSOC units like Foreign Internal Defense (FID) can target specific city areas to amplify anti-PRC sentiments at times when populations are expecting the smart city to work in a specific way (i.e., in Zhengzhou) and generate dissatisfaction to the point of spurring a small uprising that would lead to PRC companies

having to answer for their faulty technology. Using smart cities in this fashion by exploiting the management level of the kill chain could induce a change in the perception of the local populace and their behavior toward the PRC and their financial support, one that is favorable to the DOD's integrated deterrence strategy.

Second, AFSOC could directly target and attack the action level of smart cities to message or influence mass populations or targeted individuals. Digital signage, kiosks, and electronic government communications—electronic identification (eID)—are the direct vector that AFSOC can use to communicate with a local population. In Hong Kong, for example, the city has instituted eID, an application that connects the citizen and the government to provide local information, processes payments, and acts as a communication forum between the government and citizens.[131] Thus, AFSOC could deceptively send private messages to citizens on their phones using direct messages. Further, many Huawei partners produce smart city kiosks, and digital signage, to provide maps, WIFI, and charging stations. Kiosks are inherently vulnerable and open to attack because they are available 24/7 and are connected to the internet and other kiosks via a local network.[132] Therefore, an AFSOC team could remotely infiltrate or connect directly to a kiosk to access and change the output displays to help gain an information advantage.

To attack kiosks and eID applications in that manner, AFSOC can work with 16th Air Force or Special Operations Command (SOCOM) Psychological Operations officers, to place precisely targeted messages and images to inflate disinformation in advertising mechanisms to alter public opinion away from the PRC and towards the ideology of the United States. For example, such messages could be unflattering portrayals of PRC President Xi Jinping, an anti-discrimination campaign highlighting the PRC's treatment of Uighurs, or messaging promoting American technology companies while criticizing PRC companies like Huawei and Hikvision. More tactically, such actions could be misleading information to inform a local population to support localized foreign FID actions to

---

131 Victor Lam, *Building Smart Cities: An Information System Approach* (Hong Kong University: Office of the Government Chief Information Officer, 2019).

132 Denis Makrushin and Vladimir Dashchenko, *Fooling the "Smart City"* (Moscow, Russia: Kaspersky Lab, 2016), 4, https://securelist.com/fooling-the-smart-city/76060/.

generate population support. Such SEIS actions described could be coordinated, like SEAD, to gain an information advantage over PRC smart cities, and enhance the movement and maneuver of aircraft and personnel for operational necessity.

C. CONCLUSION

Because of their IADS-like capabilities, PRC smart cities present novel threats to AFSOC activities and requirements in gray-zone competition. The convergence of surveillance threats and centralized management of smart cities allow the PRC and PLA to threaten AFSOC access and movement. Denying, degrading, or increasing the risk of operating in certain areas is made possible because smart cities can directly control smart grids, thus wholly cutting off or making basic logistics and sustainment requirements like electricity, water, and internet unreliable. Further, highly advanced surveillance networks using cameras, LIDAR, and potential drone tracking, can integrate to reduce OPSEC and covertness, and prevent the movement of personnel and aircraft. This combination of technologies in an IADS-like structure reflects the potential for smart cities to double as an A2/AD weapons systems.

That said, the rapid growth, and capability of smart cities in the digital and information domains mean AFSOC can equally exploit smart cities to their benefit. The concept of SEIS, to use cyber-enabled tools in a coordinated fashion to degrade the smart cities operations and command and control through DDoS attacks like phlashing and manipulating digital twin code can help confuse city operators and PRC and PLA monitoring. The result could enable AFSOC access to airports and aerospace at reduced risk, with more covertness. Similarly, digital twin modifications can help ensure logistics and sustainment requirements are met when operationally necessitated. Finally, the same tactics combined with directly intervening in digital applications like eIDs and kiosks can produce an information advantage to influence populations and discredit the PRC's narrative in the area. The outcomes could be vital in grey-zone competition for AFSOC's access and placement.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND RECOMMENDATIONS

The PRC's proliferation of Huawei smart cities increases its centralized control of surveillance technologies, which may have potentially significant impacts on AFSOC. AFSOC personnel and aircraft rely on the ability to access and place forces, which requires logistics, sustainment, and entry to airspace. However, PRC smart cities' IADS-like structure and capabilities unlock new capabilities for the PRC and PLA to use these smart cities as weapon systems for A2/AD. However, of equal importance is that this digital environment also gives AFSOC the ability to exploit smart cities using cyber-enabled tools to disrupt the smart city kill-chain to decrease risk. Table 2 shows the A2/AD threats to and opportunities for AFSOC.

Table 2. PRC Smart City A2/AD Threats to and Opportunities for AFSOC

A2/AD Threats to AFSOC	Countering Access and Imposing Cost Opportunities
Increased Risk / Denial of Access for Movement and Maneuver: 1. Inhibiting aircraft access to airspace overtop smart cities for ISR, Fires and Mobility missions. 2. Decreased OPSEC for movement of personnel within the urban environments.	Suppression of Enemy Information Systems (SEIS): 1. Distributed Denial of Service (DDoS) attacks on vulnerable smart city infrastructure like IoT and IOCs. 2. Software hacking of- and malware placement in-digital twin for control of smart city applications.
Denial / Suppression of Logistics and Sustainment: 1. Preventing host nation supplies like water, gas, electricity, fuel, food, internet.	Detailed and sophisticated information operations to achieve an Information Advantage

This study has filled a gap and elucidates recommendations and follow-on questions/research to address and further understand the nature of PRC smart cities. Smart cities A2/AD capabilities calls for short- and long-term actions by AFSOC to maintain access and placement of forces. This list is not all-inclusive, but these recommendations will help guide AFSOC planners and tacticians to develop tactics and strategies to mitigate the threat of PRC smart cities.

A. SHORT-TERM RECOMMENDATIONS FOR AFSOC

AFSOC must prepare for potential threats and opportunities that non-military technology like smart cities can pose to grey-zone operations. In the short term, AFSOC needs to focus on four areas that can be realized using existing AFSOC resources and structures: first, developing intelligence capabilities to map the network of these smart cities and track for mission planning purposes; second, developing SEIS tactics in coordination with other major commands; third fostering new relationships with cyber and space entities and build capacity at the staff level; and fourth, educating and training to these new requirements and threats.

1. Mission Planning and Tracking Smart Cities

In the interest of maintaining operational security, and access and placement, AFSOC must aggressively pursue efforts to uncover and track PRC BRI and DSR activities to include smart cities. Further funding of Project Genghis is necessary but only scratches the surface of what is needed.[133] From an operational and tactical level, AFSOC intelligence needs to compile the locations of smart cities and should be briefed to aircrew and deploying personnel regularly. Further AFSOC Intel should develop a neural network and threat picture of PRC smart city activities that includes specific technical components of PRC smart city technologies like IOCs, IoT, AI, LIDAR, and cameras. More specifically, for each smart city, intelligence should illustrate how the smart city is connected to a more extensive global network and how the PRC may or may not have access to data in that city. Achieving this recommendation will ensure AFSOC has an accurate threat picture of all PRC activities.

2. Develop SEIS Tactics and Capabilities

To reduce the risk of smart cities to AFSOC's access and placement, AFSOC must develop new tactics suppressing smart city information systems. Chapter IV described

[133] Project Genghis, established in fiscal year 2021, is an AFSOC and SOCOM sponsored program in the Defense Analysis Department at the Naval Postgraduate School. The project focuses on cataloging and tracking the malign efforts of the PRC.

cyber and information actions that can be taken to disrupt smart cities. These concepts need to be codified into joint tactics like SEAD. AFSOC needs to leverage its Weapon School and Weapon School students to develop and codify tactics for SEIS. The result will be repeatable, trainable tactics that can be used operationally to get aircraft and personnel into areas with smart cities while preserving covertness and attribution and access and placement of AFSOC aircraft and airman. The following are important considerations in in the development of these tactics:

- Who is the supporting and supported force for these tactics? In other words, what component or command should be the lead? (Cyber, AFSOC, Space, ACC)
- What authorities are needed for conducting targeting and suppression tactics against civilian technologies and targets?
- What sort of cyber access and placement is required for SIES? Does there need to be placement of back door or dormant software technology in PRC smart cities?
- Does AFSOC need mock smart cities to train to these tactics?
- What capabilities and manning requirements does AFSOC need to conduct SEIS?

3. Manning and Integration with Cyber and Space Commands

The smart city problem set highlights the challenges that civilian technologies pose to AFSOC in the cyber, information, and space domains. AFSOC, therefore, needs to invest in technological capabilities and human capital with expertise in these areas. More staff positions incorporating cyber and space backgrounds should be created. Greater integration with Space and Cyber command calls for joint exercises to practice and develop SEIS tactics. These actions will ensure that AFSOC, from a joint perspective, comprehensively understands and is preparing for the A2/AD threats posed by smart cities.

4. Education and Training

AFSOC personnel and staff need to be prepared for interaction with PRC smart cities' and the potential threats they create. Therefore, education and training events need to be created so that AFSOC can maintain access and placement and be ready for this interaction. The following is a list of topics that these events should include:

- Biometric surveillance
- Smart grids and their impacts on operations
- Authorities for engaging civilian technologies
- Living off the Grid
- Force structuring to reduce risk of smart city A2/AD
- Cyber and space tools and tactics

B. LONG-TERM AFSOC INVESTMENTS

Simultaneously, AFSOC needs to make long-term investments in developing the capacity to counter PRC smart cities and thereby future tactics and capabilities to impose costs on the PRC. As PRC smart cities proliferate, the risk exponentially increases that smart grids will control traditional logistics and sustainment requirements. In addition, technologies like aircraft identification and anti-drone technology will continue to proliferate. Long-term, AFSOC should fund three areas: first, researching cost-effective and logistically feasible ways for deployed teams to live off the grid; second, rapidly developing COTS technology to make any aircraft in the world an AFSOC aircraft; and third, developing techniques to hide in plain sight by defeating biometric and aircraft detection technologies.

1. Research Living off the Grid: Fund Projects like ARCWATER

To prevent smart cities from disrupting or denying AFSOC logistics and sustainment requirements, it must fund further research efforts to "live off the grid" and reduce its reliance on host-nation support for logistics and sustainment requirements like

water, food, electricity, and fuel. For example, the Spark Tank winner for 2022 was Project ARCWATER, which developed a concept for allowing airmen to live off the grid using solar panels and water harvesters.[134] The portability of this technology mitigates vulnerability to smart grids while requiring 60% less space and is 74% lighter than traditional sustainment equipment like power generators.[135] However, these concepts need further refinement and funding, especially for the tactical execution of concepts like agile combat employment (ACE). The following are important considerations in the development of these tactics:

- Does the technology exist to use aircraft for power generation? Can we put solar panels and other power generators on aircraft to save electricity for ground operations?
- Can we reduce fuel requirements for aircraft? What technology is needed to make AFSOC aircraft more fuel-efficient?
- Can AFSOC invest or partner with mobility platforms that do not rely on fuel?
- What technology is needed to development new self-network connectivity that is smaller and more mobile—for example, a rapidly deployable 5G network?

2. Rapidly Develop COTS Technology to Fly Aircraft Anywhere

AFSOC aircraft stick out like a sore thumb, both visually and digitally. The centralized control of PRC smart cities threatens AFSOC's access to airspace around and above smart cities. To maintain a level of covertness for ISR and have the correct digital equipment to gain access to this airspace, AFSOC needs to continue developing commercial off-the-shelf technology to make any aircraft in the world a weapon system.

---

[134] Greg Hadley, "Spark Tank 2022: Plan to Save Water, Fuel Crowned Winner," *Air Force Magazine*, March 5, 2022, https://www.airforcemag.com/air-force-spark-tank-2022-plan-to-save-water-fuel-crowned-winner/.

[135] Hadley.

The ability to roll on and roll off a "digital pilot" would give AFSOC the ability to take an aircraft certified to fly in the smart city airspace and enable it to gain access to ISR missions. This sort of technology would preserve the covertness of the mission but reduce the risk of airspace denial and attribution to the desired mission.

3. Explore Techniques to Defeat Biometric Sensing and Aircraft Detection

AFSOC should lead the DOD in developing techniques that can defeat biometric sensing and aircraft detection. How can we hide in plain sight? There are already efforts underway to defeat biometric sensing via AI; for instance, using deep fakes is one avenue. However, how can we amplify that concept to insert not just one individual or small team but an entire AFSOC squadron? Further, how can we extrapolate those concepts to aircraft? Can we create a cloaking device that makes AFSOC aircraft virtually undetectable in the smart city?

- Can aircraft be painted or produce a specific emission control (EMCON) to deceive or defeat biometric and aircraft detection?
- Is deep fake technology capable of deceiving smart city facial recognition on the scale of an entire squadron?
- Does AFSOC and the joint force need to place backdoor or dormant software technology in smart cities to defeat such biometric abilities?

C. CONCLUSION

While smart cities are civilian technologies traditionally discussed in light of economic competition between the United States and the PRC, the United States military will have increased interaction with these systems. The omnipresence of PRC surveillance technology integrated into smart cities in an IADS-like fashion promises to challenge AFSOC's ability to access and place forces in theaters around the globe. PRC smart cities possess a sophisticated architecture that centralizes control of surveillance data and mimics a traditional military system of systems like the IADS. Technologies like IOCs, digital twin, facial recognition, traffic cameras, LIDAR, and smart grids integrate in a way familiar

to Air Force intelligence and present opportunities for exploitation by AFSOC to ensure access and placement.

This thesis has begun a conversation about BRI and DSR systems like smart cities, identifying A2/AD threats enabled by PRC smart cities' integration in a centralized manner, like an IADS, which can be weaponized against AFSOC. To the degree that the PLA can access data from Huawei smart cities globally, they give the PRC a new weapons system. That weapon system can be used to increase the risk for AFSOC accessing placing forces by hindering its movement and maneuver and sustainment and logistics access.

AFSOC and the larger joint force have rightly been focused on larger, more sophisticated air defense systems that the PRC has developed. Now is the time for AFSOC to understand and develop capabilities to exploit PRC smart cities to impose a cost on the PRC and ensure that its access and placement go unhindered. The IADS-like capabilities of smart cities give AFSOC the unique ability to develop SEIS tactics while conducting information operations to increase the cost to the PRC. Focusing on this chapter's short-term recommendations can direct AFSOC immediately in an appropriate direction. Long-term investment by AFSOC needs to research and fund projects to provide airmen and aircraft with the necessary technological capabilities to survive in these environments and reduce risk to mitigate the potential A2/AD effects of PRC smart cities. With a focus on PRC technology systems like smart cities, AFSOC can be prepared for the future grey-zone competition with the PRC.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Africa Times. "President Confirms Fatalities in Kenya Terror Attack." January 15, 2019. https://africatimes.com/2019/01/15/police-confirm-casualties-in-kenya-hotel-terror-attack/.

Air Force Special Operations Command. *AFSOC Strategic Guidance*. Hurlburt Field, FL: Air Force Special Operations Command, 2020. https://media.defense.gov/2020/May/26/2002305551/-1/-1/1/AFSOC%20STRATEGIC%20GUIDANCE.PDF.

Andrus, Heather. "Creating the Smart City Through IOT-Based Retrofitting." *U.S. Tech Online*, 2017. http://www.us-tech.com/RelId/1764960/pagenum/2/ISvars/default/Creating_the_Smart_City_through_IoT_Based_Retrofitting.htm.

Appleton, Joe. "What Is IoT and Why Is It Important for Smart Cities?" *Bee Smart City* (blog). 2021. https://hub.beesmart.city/en/solutions/what-is-iot-and-why-is-it-important-for-smart-cities.

Arquilla, John. "The Strategic Implication of Information Dominance." *Strategic Review*, 1994, 24–30. http://hdl.handle.net/10945/41668.

Atha, Katherine, Jason Callahan, John Chen, Jessica Drun, Green Kieran, Brian Dr. Lafferty, Joe McReynolds, James Mulvenon, Benjamin Rosen, and Emily Walz. *China's Smart Cities Development*. Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission. Vienna, VA: SOS International, 2020. https://www.uscc.gov/sites/default/files/2020-04/China_Smart_Cities_Development.pdf.

Bartholomew, Carolyn. "China and 5G." *Issues in Science and Technology* 36, no. 2 (Winter 2020): 50–57. http://www.proquest.com/docview/2452125915/abstract/CA8F81FEDAB413DPQ/1.

BBC. "Safe Cities: Using Smart Tech for Public Security." Accessed November 1, 2021. http://www.bbc.com/future/bespoke/specials/connected-world/government.html.

Blackman, James. "China Unicom, Huawei Test 5G 'Super Sensing' for Drones, Transport, Digital Twins." Enterprise IoT Insights, December 17, 2021. https://enterpriseiotinsights.com/20211217/channels/news/china-unicom-huawei-combine-on-5g-super-sensing-for-drone-detection-road-transport.

Bronk, Justin. "Modern Russian and Chinese Integrated Air Defense Systems: The Nature of the Threat, Growth Trajectory and Western Options." *Royal United Services Institute*, January 15, 2020. https://rusi.org/explore-our-research/publications/occasional-papers/modern-russian-and-chinese-integrated-air-defence-systems-nature-threat-growth-trajectory-and.

Chen, John, Emily Walz, Brian Lafferty, Joe McReynolds, Kieran Green, Jonathan Ray, and James Mulvenon. *China's Internet of Things*. Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission. Vienna, VA: SOS International, 2018. https://www.uscc.gov/sites/default/files/Research/SOSi_China's%20Internet%20of%20Things.pdf.

Collier, Chelsea. "What a Smart City Is… and Is Not – Smart Cities Connect." Smart Cities Connect Media & Research, January 27, 2020. https://smartcitiesconnect.org/what-a-smart-city-is-and-is-not/.

Creemers, Rogier. "National Cyberspace Security Strategy." *China Copyright and Media* (blog). December 27, 2016. https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/.

Dameri, Renata Paola, and Camille Rosenthal-Sabroux. "Smart City and Value Creation." In *Smart City: How to Create Public and Economic Value with High Technology in Urban Space*, 1–12. Progress in IS. Cham: Springer International Publishing, 2014. https://doi.org/10.1007/978-3-319-06160-3_1.

Dekker, Brigitte, Maaike Okano-Heijmans, and Eric Siyi Zhang. *Unpacking China's Digital Silk Road*. Clingendael Institute, 2020. https://www-jstor-org.libproxy.nps.edu/stable/resrep25693.

Department of the Air Force. *Counterair Operations*. AFDP 3–01. Maxwell AFB, Montgomery, AL: Air University, 2019. https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-01/3-01-AFDP-D02-AIR-Counterair-Operations.pdf.

Deren, Li, Yu Wenbo, and Shao Zhenfeng. "Smart City Based on Digital Twins." *Computational Urban Science* 1, no. 1 (March 29, 2021): 11. https://doi.org/10.1007/s43762-021-00005-y.

Diender, Edwin. "Why One Connected City Is Not a Connected City." *Huawei* (blog). September 11, 2020. https://blog.huawei.com/2020/09/11/why-one-connected-city-not-connected-city/.

Dossi, Simone. "On the Asymmetric Advantages of Cyberwarfare. Western Literature and the Chinese Journal Guofang Keji." *Journal of Strategic Studies* 43, no. 2 (February 23, 2020): 281–308. https://doi.org/10.1080/01402390.2019.1581613.

Dou, Eva. "Huawei Documents Show Chinese Tech Giant's Involvement in Surveillance Programs." *The Washington Post*, December 14, 2021. https://www.washingtonpost.com/world/2021/12/14/huawei-surveillance-china/.

Dougherty, Chris. "Moving Beyond A2/AD." Center for New American Security, December 3, 2020. https://www.cnas.org/publications/commentary/moving-beyond-a2-ad.

Ekman, Alice. “China’s Smart Cities: The New Geopolitical Battleground.” *Etudes de L’Ifri*, December 2019. https://www.ifri.org/sites/default/files/atoms/files/ekman_smart_cites_battleground_2019.pdf.

Francois, N.D. “Huawei’s Surveillance Tech in Kenya: A Safe Bet?” *Africa Times*, December 17, 2019. https://africatimes.com/2019/12/18/huaweis-surveillance-tech-in-kenya-a-safe-bet/.

Frost, Adam. “Lidar Sensors for Combined Smart City and Av Ecosystem.” *Traffic Technology Today*, December 11, 2019, sec. Smart Cities. https://www.traffictechnologytoday.com/news/smart-cities/lidar-sensors-for-combined-smart-city-and-av-ecosystem.html.

Hadley, Greg. “Spark Tank 2022: Plan to Save Water, Fuel Crowned Winner.” *Air Force Magazine*, March 5, 2022. https://www.airforcemag.com/air-force-spark-tank-2022-plan-to-save-water-fuel-crowned-winner/.

Halegoua, Germaine R. *Smart Cities*. MIT Press Essential Knowledge Series. Cambridge, Massachusetts: MIT Press, 2020.

Hemmings, John. “Reconstructing Order: The Geopolitical Risks in China’s Digital Silk Road.” *Asia Policy* 15, no. 1 (January 2020): 5–21. http://www.proquest.com/docview/2355329399/abstract/E77E9684AC724836PQ/2.

Hillman, Jennifer, and David Sacks. *China’s Belt and Road: Implications for the United States*. Independent Task Force, No. 79. New York, NY: Council on Foreign Relations, 2021. https://www.cfr.org/report/chinas-belt-and-road-implications-for-the-united-states/.

Hillman, Jonathan. “Disrupting China’s Digital Silk Road.” Presentation, National Defense University, March 31, 2021. https://nsiteam.com/disrupting-chinas-digital-silk-road/.

———. *The Emperor’s New Road: China and the Project of the Century*. New Haven: Yale University Press, 2020.

Hu, Richard. “The State of Smart Cities in China: The Case of Shenzhen.” *Energies* 12, no. 22 (January 2019): 4375. https://doi.org/10.3390/en12224375.

Huai, Zhang. “How Big Data and AI Will Transform Shenzhen Airport.” Huawei. Accessed December 15, 2021. https://www.huawei.com/en/technology-insights/publications/winwin/32/shenzhen-airport-digital-platform-and-ai.

Huawei. “Building Happier Smart Cities.” Accessed April 13, 2022. https://e.huawei.com/en/publications/global/ict_insights/ict31-digital-government/comment/smart-cities-that-provide-a-Sense-of-security.

———. *Building the Future: New ICT Enables Smart City*. Huawei. Alexandria, VA: IDC Government Insights, 2017. https://e.huawei.com/en/material/industry/smartcity/9b0000e57fa94a2dbc0e43f5817ca767.

———. “Huawei Announces Collaboration with Honeywell to Develop Smart Building Offerings.” March 22, 2017. https://www.huawei.com/en/news/2017/3/Huawei-Honeywell-Smart-Building-Offerings.

———. “Huawei Creates a Smart City Nervous System for More Than 100 Cities with Leading New ICT.” November 14, 2017. https://www.huawei.com/en/news/2017/11/Huawei-Smart-City-Nervous-System-SCEWC2017.

———. “Huawei Integrated ITS Cameras.” Accessed November 18, 2021. https://e.huawei.com/en/products/intelligent-vision/cameras/software-defined-camera/electric-police-bayonet.

———. “Huawei Smart City Overview Presentation.” Presentation. June 10, 2018. https://e.huawei.com/en/material/industry/smartcity/02ad4d5ab608492ea24659ec667f04bd.

———. “Huawei Vehicle Cameras.” Accessed November 18, 2021. https://e.huawei.com/en/products/intelligent-vision/cameras/software-defined-camera/vehicle-micro-checkpoint.

———. “Intelligent Operation Center Solution.” Accessed November 1, 2021. https://e.huawei.com/en/solutions/industries/government/smart-city/ioc.

———. “Leading New ICT, Building a Smart City Brain.” Accessed September 18, 2021. https://e.huawei.com/en/material/industry/smartcity/fd6fc58e324a4beba385fc00672e75a7.

———. “Powering the Future with Smart Grids.” Accessed April 13, 2022. https://www.huawei.com/en/technology-insights/publications/winwin/plus-intelligence/powering-the-future-smart-grids.

———. “Smart City.” Accessed April 20, 2021. https://e.huawei.com/en/solutions/industries/government/smart-city.

———. “Smart City-Facilitating the Upgrade of City Infrastructure, Management, and Services.” Accessed November 14, 2021. https://www.huaweicloud.com/intl/en-us/solution/smartcity.html.

———. “What Is a Software-Defined Camera?” Accessed November 14, 2021. https://e.huawei.com/en/products/intelligent-vision/cameras/software-defined-camera.

Jinping, Xi. *Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era*. Beijing, China: Xinhua News, 2017. http://www.xinhuanet.com/english/download/Xi_Jinping's_report_at_19th_CPC_National_Congress.pdf.

Joint Chiefs of Staff. *Joint Forcible Entry Operations*. JP 3-18. Washington, DC: Joint Chiefs of Staff, 2017. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_18ch1.pdf.

———. *Joint Operations*. JP 3-0. Washington, DC: Joint Chiefs of Staff, 2017. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf.

Joint Staff Joint Force Development and Design Directorate (J-7). *Irregular Warfare Mission Analysis*. Washington, DC: Joint Chiefs of Staff, 2021.

Jones, Mason P., and Erica L. McCaslin. "Special Operations in a 5G World: Can We Still Hide in the Shadows?" Master's thesis, Monterey, CA; Naval Postgraduate School, 2020. https://calhoun.nps.edu/handle/10945/65560.

The Kenya Alliance of Resident Associations. "Kenya Fights Insecurity with Technology." June 17, 2016. https://karakenya.wordpress.com/2016/06/17/kenya-fights-insecurity-with-technology/.

Khan, Sulmaan Wasif. *Haunted by Chaos: China's Grand Strategy from Mao Zedong to Xi Jinping*. Cambridge, MA; London, England: Harvard University Press, 2018.

Kumar, Vivek. "What AI and Machine Learning Can Do for a Smart City?" Analytics Insight, December 7, 2019. https://www.analyticsinsight.net/ai-machine-learning-can-smart-city/.

Lam, Victor. *Building Smart Cities: An Information System Approach*. Hong Kong University: Office of the Government Chief Information Officer, 2019.

Lee, Sangkuk. "China's 'Three Warfares': Origins, Applications, and Organizations." *Journal of Strategic Studies* 37, no. 2 (February 23, 2014): 198–221. https://doi.org/10.1080/01402390.2013.870071.

Liang, Qiao, and Wang Xiangsui. *Unrestricted Warfare*. Medina University Press International, 2021. Kindle.

Lida, Yan. "Creating a Smart City 'Nervous System.'" *ICT Insights*, August 2018. https://e.huawei.com/en/publications/global/ict_insights/201806041630/commentary/201807131639.

Lu, Dong, Ye Tian, Vincent Y. Liu, and Yi Zhang. "The Performance of the Smart Cities in China—A Comparative Study by Means of Self-Organizing Maps and Social Networks Analysis." *Sustainability* 7, no. 6 (2015): 7604–21. http://dx.doi.org/10.3390/su7067604.

Maizland, Lindsay, and Andrew Chatzky. "Huawei: China's Controversial Tech Giant." Council on Foreign Relations, August 6, 2020. https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant.

Makrushin, Denis, and Vladimir Dashchenko. *Fooling the "Smart City."* Moscow, Russia: Kaspersky Lab, 2016. https://securelist.com/fooling-the-smart-city/76060/.

Meegan, Daniel. "Breaking Other People's Toys: Sabotage in a Multipolar World." Master's thesis, Monterey, CA; Naval Postgraduate School, 2020. https://calhoun.nps.edu/handle/10945/66686.

National Geographic. "Smart Cities." April 10, 2020. http://www.nationalgeographic.org/article/smart-cities/.

Office of the Director of National Intelligence. *Annual Threat Assessment of the U.S. Intelligence Community*. Section 617 of P.L. 116–260. Washington, DC: Director of National Intelligence, 2021. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.

Pan, Che, and Masha Borak. "Did Zhengzhou's Much-Hyped Smart City Projects Fail to Prevent the Floods?" *South China Morning Post*. July 28, 2021, sec. Big Tech. https://www.scmp.com/tech/big-tech/article/3142898/china-floods-smart-city-system-capabilities-called-question-after.

People's Daily Online. "Xi Calls for Making Major Cities 'Smarter.'" April 1, 2020. http://en.people.cn/n3/2020/0401/c90000-9674926.html.

Pisani, Kate. "'Open Sesame': Identifying China's Cyberspace Vulnerabilities." Master's thesis, Monterey, CA; Naval Postgraduate School, 2019. https://calhoun.nps.edu/handle/10945/64048.

Reichert, Corinne. "US Finds Huawei Has Backdoor Access to Mobile Networks Globally, Report Says." CNET. Accessed March 10, 2022. https://www.cnet.com/tech/mobile/us-finds-huawei-has-backdoor-access-to-mobile-networks-globally-report-says/.

Sanger, David, and Emily Schmall. "China Appears to Warn India: Push Too Hard and the Lights Could Go Out." *The New York Times*, September 27, 2021. https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html.

Sharma, Neeta, Mahtab Alam, and Mayank Singh. “Denial of Service: Techniques of Attacks and Mitigation.” *Journal of Computer Science Engineering and Software Testing* 1, no. 2 (July 1, 2015): 11–14. https://www.researchgate.net/profile/Neeta-Sharma-7/publication/296561817_Denial_of_Service_Techniques_of_Attacks_and_Mitigation/links/56d6987908aebabdb400c5d9/Denial-of-Service-Techniques-of-Attacks-and-Mitigation.pdf.

Smith, Bryan F. “A Model of an Integrated Air Defense System (IADS) for the Tacops Program.” Thesis, Monterey, California. Naval Postgraduate School, 1991. https://calhoun.nps.edu/handle/10945/26640.

UAS Traffic Management News. “Huawei and Unifly to Work Together on Drone ID and Tracking UTM Integration.” June 11, 2018. https://www.unmannedairspace.info/uncategorized/huawei-unifly-work-together-drone-id-tracking-utm-integration/.

Valeriano, Brandon, Benjamin Jensen, and Ryan Maness. “China and the Technology Gap: Chinese Strategic Behavior in Cyberspace.” In *Cyber Strategy: The Evolving Character of Power and Coercion*. Ryan. New York, N.Y., United States: Oxford University Press, 2019.

Weekes, Sue. “The Rise of Digital Twins in Smart Cities.” Smart Cities World, January 6, 2019. https://www.smartcitiesworld.net/special-reports/special-reports/the-rise-of-digital-twins-in-smart-cities.

Wei, Low De. “Why the Solomon Islands’ China Pact Has U.S. Riled.” Bloomberg, April 22, 2022. https://www.bloomberg.com/news/articles/2022-04-22/why-the-solomon-islands-china-pact-has-u-s-riled-quicktake.

Xinhua News. “National New-Type Urbanization Plan (2014-2020).” March 16, 2014. http://www.gov.cn/zhengce/2014-03/16/content_2640075.htm.

Yap, Chuin-Wei. “State Support Helped Fuel Huawei’s Global Rise.” *The Wall Street Journal*, December 25, 2019, sec. Tech. https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.

Yong, Pei. “Intelligent Operations Center: A Smart Brain for City Management.” *ICT Insights*, November 2019. https://e.huawei.com/en/publications/global/ict_insights/201908281022/focus/201911081641.

Yu, Wenxuan, and Chengwei Xu. “Developing Smart Cities in China: An Empirical Analysis.” *International Journal of Public Administration in the Digital Age (IJPADA)* 5, no. 3 (2018): 76–91. https://doi.org/10.4018/IJPADA.2018070106.

Zhiwei, Zhang. “Huawei Consolidates the Foundation of Smart Cities.” *ICT Insights*, August 2018. https://e.huawei.com/en/publications/global/ict_insights/201806041630/special-report/201808170832.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California