
From AFIO's THE INTELLIGENCER
JOURNAL OF U.S. INTELLIGENCE STUDIES
VOLUME 28 • NUMBER 1 • Winter-Spring 2023 $15 SINGLE COPY PRICE

Association of Former Intelligence Officers
7600 Leesburg Pike, Suite 470 East
Falls Church, Virginia 22043
Web: www.afio.com * E-mail: afio@afio.com

STUDENT ARTICLE

Pervasive Threats to U.S. National Security from Chinese Tech Companies[1]

by Jason A. Harriman
First Lieutenant, US Army

Since the invention of modern computers and the internet that connects them, technology has become a huge part of American society; so much so that we have become reliant on the conveniences that technology provides. The proliferation of cheaply made electronics from China presents unique security threats that the average American is unprepared to mitigate; not because of the component's quality, but because it is highly likely that the Chinese government has the pronounced ability to access the information passing through these components according to multiple government sources, especially the FCC, and coinciding with Huawei's ban in the United States. China's Belt and Road Initiative (CBRI) can be cited as the driver for this technology's rapid proliferation throughout the world. Chinese technology has become a key component in what is known as "Smart Cities," especially in low-income countries where their lower prices are very attractive. Lastly, 5G networks may present increased capabilities for American adversaries in the realm of intelligence collection, and an added dimension that Foreign Intelligence Entities can exploit.

China has relatively recently returned to its place as a world power following its defeat by western powers in the 19th century and nearly by Japan in World War Two. The Chinese have chosen to pursue power in ways that are confrontational and often conflict with the interests of the Western nations, namely the United States. China dominates the global telecommunications industry, especially in developing nations, by manufacturing adequate components at a fraction of the cost of non-Chinese competitor companies due to government subsidies and the China Belt and Road Initiative (CBRI).

The Chinese government's ability to access the information stored on and passing through their commercially sold technology designed and manufactured by Chinese companies, threatens not only the security of the United States and its individual citizens, but the security of the any country who agrees to allow Chinese technology within its communications networks. This threat coincides with the ban on Huawei, ZTE, and others being allowed to sell their products in the United States and other allied nations. The CBRI has largely driven this technology's rapid proliferation throughout the world and thus has made it a global security threat. Lastly, if Chinese technology continues to drive the future of 5G telecommunications network development, it will likely present a greater threat to the United States both at home and abroad.

The FCC has come to similar conclusions regarding the below research questions. The contribution to the national security and counterintelligence (CI) field from this paper, is further and deeper research to confirm the FCC report, as well as to provide more nuanced information that relates to both the Intelligence Community, as well as to policy makers seeking to harden U.S. cyber defenses. The Intelligence Community-related material concerns mostly sub-question #2; in that the information most at risk is also the information that should be protected most fiercely from a CI field perspective. The information most relevant to the policy maker, is both the reaffirmation of the FCC's findings and additional DoD security advisories (the main research question), and sub-question #1. Answering sub-question #1, will allow policy makers to make educated decisions about the future of U.S. networks, and about partnerships with other nations who could be at risk if they are using Chinese equipment.

RESEARCH QUESTIONS

In this research paper – and as a continuation of research on the topic from previous theses – I want to explore the following main question, as well as sub-questions to provide context. This paper seeks to answer questions that are valuable at both the senior policymaker level, down to the individual warfighter level.

1. The statements of fact, opinion, or analysis expressed in this document are strictly my own [or those of the author] and do not reflect the official policy or position of the Department of Defense (DoD), or the U.S. Government. Review of the material does not imply DoD or U.S. Government endorsement of factual accuracy or opinion.

- Main Question: How does the use of Chinese commercially made telecommunications equipment affect the probability of compromise by Chinese Intelligence Services, and could other brands'/countries' products be just as vulnerable?
- Sub-Question #1: What telecommunications components are most likely to be compromised by Chinese Intelligence Services (broadly) both prior to product purchase (e.g., -preloaded backdoor), and after network installation (e.g., brute force hacking, signals intelligence collection, etc.)?
  - Assumptions: Chinese companies almost certainly install backdoor access into the software and hardware they design and manufacture primarily for maintenance purposes; other purposes are possible.
- Sub-Question #2: How might China use intelligence collected while transiting networks containing critical components (hardware/software) designed and manufactured in China?
  - Assumptions: China has both the capability and intent to access the data flowing through telecommunications network components, especially those designed and manufactured by Chinese companies.
  - China believes there is intelligence of value to be gained from surveilling telecommunications network data.

MODERN RELEVANCE

Market research company Frost & Sullivan estimates through exhaustive research, that 80% of the world's population in developed countries will reside in urban cities by the year 2050, and that figure reaches more than 60% in current developing nations. Other research companies such as Grand View Research and Allied Market Research sing a similar tune. Smart city technology will be the most effective way to manage large urban populations in the future.[2]

As was the case with the invention of modern computers and the internet, where the benefits of such devices also presented new and emerging threats/vulnerabilities, the same is presented by smart city technology. With every invention, the potential for malicious use is also present and smart cities are no different. Smart cities are quite literally designed to collect as much information as possible, direct the functions of city infrastructure as efficiently as possible and, overall to greatly improve the lives of the residents within the city limits.[3] Should any entity with malicious intent gain access to these systems that control so much of the city infrastructure, the amount of damage which could be done is immense.

As the proliferation of smart cities increases, so too will the need for literature on the topic. This paper will serve as a summary of the topic as it pertains to protecting U.S. interests and examining the counter-intelligence/intelligence threat to U.S. Interests.

REVIEW OF LITERATURE

China has relatively recently returned as a world power following multiple defeats by western powers in the 19th century and nearly by Japan in World War Two. The Chinese have chosen to pursue power in ways that are often perceived by the West as confrontational and often conflict with the interests of the Western nations, namely the United States. China dominates the global telecommunications industry, especially in developing nations, by manufacturing adequate components at a fraction of the cost of non-Chinese competitor companies due to government subsidies and the China Belt and Road Initiative (CBRI).

The Chinese government's probable ability to access the information stored on and passing through their commercially sold technology designed and manufactured by Chinese companies, threatens not only the security of the United States and its individual citizens, but the security of any country who agrees to allow Chinese technology within its communications networks. This threat coincides with the ban on Huawei, ZTE, and others being allowed to sell their products in the United States and other allied nations. The CBRI has largely driven this technology's

2. "Smart Cities: Frost and Sullivan Value Proposition," accessed April 12, 2020, *https://ww2.frost.com/wp-content/uploads/2019/01/SmartCities.pdf*; Digital Sigage Today, "Frost & Sullivan Report Global Smart Cities to Surpass $2 Trillion by 2025," *www.digitalsignagetoday.com*, April 17, 2018, *https://www.digitalsignagetoday.com/news/frost-sullivan-report-global-smart-cities-to-surpass-2-trillion-by-2025/*; Allied Market Research, "Smart Cities Market Size and Share | Industry Analysis, 2025," Allied Market Research, November 2018, *https://www.alliedmarketresearch.com/smart-cities-market*.

3. Federico Guerrini, "Are Smart Cities Really Smart?," Forbes, May 6, 2014, *https://www.forbes.com/sites/federicoguerrini/2014/05/06/the-pros-and-cons-of-smart-cities/*.you know what I'm talking about. An enormous metropolis, hyper-technological and hyper-connected (though the Internet had yet to be invented when the books were first published

rapid proliferation throughout the world and thus has made it a global security threat. Lastly, if Chinese technology continues to drive the future of 5G telecommunications network development, it will likely present a greater threat to the United States both at home and abroad.

U.S. Companies have been officially banned from using Huawei technology since 2021, but have been discouraged since at least 2012, because of concerns over the connections between Huawei execs and the Chinese Communist Party, as well as the greater Chinese government and military.[4] The company's CEO, for example, is a former research and development engineer in telecommunications and information technology for the Chinese People's Liberation Army (PLA) and experts agree that he maintains close and continuing relationships with persons inside the Chinese government, CCP, PLA, and other similar organizations.[5] Huawei, ZTE, and other lesser-known Chinese companies can each provide hardware required to integrate the technology that makes a city 'smart' into existing infrastructure.[6]

Chinese Foreign Policy

China's Belt and Road Initiative (CBRI/BRI), also known as the New Silk Road, was launched in 2013 by Chinese President Xi Jinping, creating numerous infrastructure development and investment initiatives around the world. The CBRI targets mostly developing nations, but some European countries have also signed on to China's deal seeking to upgrade their infrastructure, especially where 5G cellular networks and smart city technologies are concerned (although many developing nations are seeking 5G network capability as well).[7]

This paper views the New Silk Road as a major driver of China's increasing global power and a vehicle to carry China's foreign policy objectives, including regional development and military expansion, to their limits. The more locations that the Chinese government can access and observe, the more robust its intelligence collection apparatus becomes.[8] Big data has already proven to be a significant factor of domestic Chinese governance and is likely a significant contributor to their foreign intelligence collection as well. Smart cities utilizing 5G cellular networks, coupled with Chinese near dominance of the commercial production and sale of the components that make them, presents a significant national security threat in the near future.

The original Silk Road came about during the Chinese Han Dynasty [206 BC – 22 AD] and was a system of trade routes throughout all of Asia including the Middle East, ending in major European cities. All of this intra-regional trade allowed these countries to prosper in many respects. The Silk Road peaked right up until the Crusades and Mongol incursions westward which combined, dampened Intra-Asian trade. Today, intra-regional trade between central Asian countries is extremely low (Afghanistan, Tajikistan, Uzbekistan, Turkmenistan, Kazakhstan and Kyrgyzstan), making up only 6.2% of the total of all these countries' international trade according to the Washington International Trade Association.[9]

Projects are planned, such as railways, energy pipelines, highways, and streamlined border crossing procedures, westward—through the mountainous former Soviet republics—and southward, to Southern and Southeast Asia. These trade networks are designed to expand the international use of Chinese currency and "break the bottleneck in Asian connectivity,"

4. Rich Haridy, "Huawei, the US Ban, and Links to Chinese Spying Explained," New Atlas, May 22, 2019, *https://newatlas.com/huawei-ban-us-what-spy-evidence-exists/59772/*; Sean Keane, "Huawei Ban Timeline: Detained CFO Makes Deal with US Justice Department," CNET, accessed April 23, 2022, *https://www.cnet.com/news/privacy/huawei-ban-timeline-detained-cfo-makes-deal-with-us-justice-department/*; Russell Brandom, "The Case against Huawei, Explained," The Verge, May 22, 2019, *https://www.theverge.com/2019/5/22/18634401/huawei-ban-trump-case-infrastructure-fears-google-microsoft-arm-security*; Jon Porter, "US Delays Full Huawei Ban yet Again until May 15th," The Verge, March 12, 2020, *https://www.theverge.com/2020/3/12/21176530/huawei-us-ban-extension-length-rural-providers-network-infrastructure*; Joy Tan for CNN Business Perspectives, "Huawei Exec: The US Can't Afford to Work without Us," CNN, accessed April 23, 2022, *https://www.cnn.com/2020/02/28/perspectives/huawei-ban-5g-technology/index.html*.

5. Huawei Ltd., "Mr. Ren Zhengfei - Huawei Executives," huawei, accessed April 23, 2022, *https://www.huawei.com/us/executives/board-of-directors/ren-zhengfei*; Raymond Zhong, "Who Owns Huawei? The Company Tried to Explain. It Got Complicated.," The New York Times, April 25, 2019, sec. Technology, *https://www.nytimes.com/2019/04/25/technology/who-owns-huawei.html*.

6. opinion contributors Annie Fixler and Mikhael Smits, "Huawei Endangers Western Values," Text, The Hill (blog), January 24, 2020, *https://thehill.com/opinion/cybersecurity/479748-huawei-endangers-western-values/*.

7. Danielle Cave, "The African Union Headquarters Hack and Australia's 5G Network," The Strategist, July 12, 2018, *https://www.aspistrategist.org.au/the-african-union-headquarters-hack-and-australias-5g-network/*; James McBride and Andrew Chatzky, "China's Massive Belt and Road Initiative," Council on Foreign Relations, accessed April 23, 2022, *https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative*; James McBride, "Building the New Silk Road," Council on Foreign Relations, accessed April 23, 2022, *https://www.cfr.org/backgrounder/building-new-silk-road*; Marguerite Reardon, "Nokia and Ericsson Pitch Themselves as Huawei 5G Alternative," CNET, accessed April 23, 2022, *https://www.cnet.com/tech/mobile/nokia-and-ericsson-pitch-themselves-as-huawei-5g-alternative/*.

8. OOKLA, "Ookla 5G Map - Tracking 5G Network Rollouts Around the World," accessed April 23, 2022, *https://www.speedtest.net/ookla-5g-map*.

9. McBride, "Building the New Silk Road"; Wilson Center, "The New Silk Road Initiative Post-2014: Challenges and Opportunities | Wilson Center," accessed April 23, 2022, *https://www.wilsoncenter.org/event/the-new-silk-road-initiative-post-2014-challenges-and-opportunities*.

according to Chinese President Xi Jinping. The Asian Development Bank estimates that these regional projects face a severe infrastructure financing gap of roughly $800 billion. While no official list exists for participants in the CBRI, the initiative involves more than 60 countries, many of whom are close economic and military partners with the United States.[10]

The largest single project planned so far is the $68 billion China-Pakistan Economic Corridor. This is a system of projects connecting roads and rails from Chinese industrial centers to Pakistan's Gwadar Port on the Arabian Sea. It is estimated that China has spent more than $200 billion on this and other efforts in the region. Morgan Stanley - an American multinational investment bank and financial services company – has predicted China's cumulative investment in the CBRI could reach $1.2–1.3 trillion by 2027. However, it is worth noting that this figure varies based on the source as some organizations doubt that China has the ability or will to pay that much over that short of a timespan.[11]

Many countries have voiced their displeasure of the CBRI, especially the United States and some of their allies. Many countries have taken on massive loans from Chinese banks as opposed to aid grants to fund infrastructure projects which are also performed by Chinese Labor, and Chinese-State owned companies. Some CBRI projects contain a loosely worded bidding process which requires the use of Chinese companies to fulfill the loan. Because of this, Chinese construction companies vastly inflate the costs which results in canceled projects as well as political backlash to the project hosting country.[12]

Predatory Debt Traps

There are other serious concerns surrounding these seemingly limitless loans as well. A 2018 report from the Center of Global Development denotes eight countries enrolled in CBRI projects are "vulnerable to debt crises."[13] Overall global debt to China has increased significantly since the CBRI was announced and shows that in some at risk countries, indebtedness to China is often more than 20% of their GDP. Chinese banking practices to these countries is in many ways, predatory; giving out loans to developing countries without significant regard to their ability to pay up.[14] Should a country indebted to China get into a no-pay situation, it could be used by the CCP to influence, coerce, or even blackmail countries to "toe-the-line."

This practice is called a "Debt Trap." According to the New York Times, China has financed more than 35 ports around the world, mostly in Africa and Asia, but a least one off the coast of Florida in the Bahamas. Sri Lanka is a shining example of a debt trap conceived by China. The Sri Lankan port, Hambantota resides in one of the busiest sectors of worldwide shipping lanes in the world with thousands of ships passing by every year and yet, in 2012, they drew in only 34 ships. One of many loans granted by China to Sri Lanka, was used to renovate the port. In short, Sri Lanka defaulted on their loan, and now the Chinese government has a 99-year lease on the port, as well as 15000 acres of land surrounding it. The port is used for both civilian and military purposes however, it is significantly valuable to the Chinese because of its proximity to one of their rivals, India.[15]

Chinese Intelligence and Cybersecurity Law

In 2017, China passed a series of tech-oriented laws aimed at increasing the protection granted to consumers from private companies, while simultaneously increasing the legal power that the Chinese government has to surveil. These laws which grant more power to the Chinese government, could be used as a basis to force companies like Huawei and ZTE to provide access or turn over stored data flowing through their hardware from anywhere in the world (re: Case Study: African Union HQ Breach).

The 2017 National Intelligence Law gives authorities sweeping powers to monitor and investigate foreign and domestic individuals and institutions. It allows Chinese intelligence agencies to search premises, seize property, and mobilize individuals or organizations to carry out espionage. It also gives

10. McBride and Chatzky, "China's Massive Belt and Road Initiative"; McBride, "Building the New Silk Road"; WTZ, "5G Commercial Network in 2019 World Coverage Map - 5G Country List - 5G Networks around the World - Countries with World Coverage 5G Network Technology Country List," accessed April 23, 2022, *https://www.worldtimezone.com/5g.html*.

11. McBride and Chatzky, "China's colossal infrastructure investments may usher in a new era of trade and growth for economies in Asia and beyond. But skeptics worry that China is laying a debt trap for borrowing governments."Council on Foreign Relations, *China's Massive Belt and Road Initiative*. See: *https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative*, accessed 23 April 2023.

12. Maria Abi-Habib, "How China Got Sri Lanka to Cough Up a Port," The New York Times, June 25, 2018, sec. World, *https://www.nytimes.com/2018/06/25/world/asia/china-sri-lanka-port.html*.

13. China Development Bank, "China Development Bank," accessed April 23, 2022, *http://www.cdb.com.cn/English/gykh_512/khjj/*; Catherine Trautwein, "All Roads Lead to China: The Belt and Road Initiative, Explained," FRONTLINE, accessed April 23, 2022, *https://www.pbs.org/wgbh/frontline/article/all-roads-lead-to-china-the-belt-and-road-initiative-explained/*.

14. Trautwein, "All Roads Lead to China."

15. Abi-Habib, "How China Got Sri Lanka to Cough Up a Port."

intelligence agencies legal ground to carry out their work both within and outside China. So, while the people are more protected data-wise from private companies who may seek to exploit their personal information for their own gain, everyone becomes less secure from the Chinese government.

National Security Law of 2017 and The People's Republic of China Cyber Security Law

Articles 11, 12, and 14 of China's 2017 National Intelligence Law, and Article 28 of the Cybersecurity Law, are of particular interest to this paper as they appear to grant the most power to Chinese intelligence and law enforcement agencies. The full text of these laws is below and translated from Chinese.[16]

> Article 11: National intelligence work institutions shall lawfully collect and process relevant intelligences on foreign bodies, organizations and individuals engaged in, or inciting or assisting others to engage in, or domestic bodies, organizations and individuals who collude with foreign bodies, organizations or individuals to engage in harm to the national security and interests of the People's Republic of China, in order to provide intelligence as a reference and basis and reference for preventing, curbing and punishing the above acts.[17]

In summary, Article 11 grants Chinese authorities permission to spy on anyone and everyone they deem a threat to their national security or who they have any suspicion of working against their interests. It also grants Chinese authorities the ability to "[prevent, curb, and punish]" those who are found guilty of the above actions. This would be of particular concern to anyone who speaks in opposition of the CCP, spies, businesses operating in China, foreign diplomatic delegations, and even put at risk tourists the CCP sees as suspicious.

> Article 12: National intelligence work institutions may, according to relevant state regulations, establish cooperative relationships with relevant individuals and organizations, and commission them to carry out related work.[18]

Article 12 encourages intelligence and law enforcement agencies to work with private companies and organizations – like Huawei and ZTE, but not limited to domestic companies – to accomplish their intelligence collection objectives. It even allows the state to employ these companies and direct them to enable their intelligence collection (as is potentially/probably the case in the AU case study) or even collect intelligence on their behalf.

> Article 14: National intelligence work institutions, when carrying out intelligence work according to laws, may ask relevant institutions, organizations and citizens to provide necessary support, assistance and cooperation.[19]

Article 14 essentially grants the state the ability to question any individual, company, or organization they wish to assist or support any type of investigation. The law does not explicitly require the questions to be answered. However, China does not have an equivalent to the United States' 4th and 5th Amendments, which protect U.S. Persons from unreasonable searches and seizures and guarantees both due process of law and a right against self-incrimination. In fact, Article 93 of the Chinese Criminal Procedure Law ensures that criminal suspects must answer all relevant questions truthfully and may "have the right to refuse to answer any questions that are irrelevant to the case" thus virtually eliminating the "right to remain silent." To that end, when Chinese authorities 'ask' questions, a truthful response is compulsory.

16. Tanner, M. (2017, July 20). Beijing's New National Intelligence Law: From Defense to Offense. Retrieved April 23, 2022, from https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense

17. "Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," New America, accessed April 23, 2022, *http://newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/*; Murray Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," Lawfare, July 20, 2017, *https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense*; Courtney Bowman, Lijuan Hou, and Ying Li, "A Primer on China's New Cybersecurity Law: Privacy, Cross-Border Transfer Requirements, and Data Localization," Privacy Law Blog, May 9, 2017, *https://privacylaw.proskauer.com/2017/05/articles/cybersecurity/a-primer-on-chinas-new-cybersecurity-law-privacy-cross-border-transfer-requirements-and-data-localization/*; People's Republic of China, "Cybersecurity Law of the People's Republic of China" (Effective June 1, 2017)," DigiChina (blog), accessed April 23, 2022, *https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/*.

18. Tanner, "Beijing's New National Intelligence Law"; Bowman, Hou, and Li, "A Primer on China's New Cybersecurity Law"; People's Republic of China, "Translation." China's National Intelligence Law, enacted on June 27 with unusual speed and limited public discussion, is a uniquely troubling milestone in Beijing's four-year-old campaign to toughen its security legislation. Like the more widely reported Cybersecurity Law (which went into effect on June 1).

19. Tanner, "Beijing's New National Intelligence Law"; Bowman, Hou, and Li, "A Primer on China's New Cybersecurity Law"; People's Republic of China, "Translation." China's National Intelligence Law, enacted on June 27 with unusual speed and limited public discussion, is a uniquely troubling milestone in Beijing's four-year-old campaign to toughen its security legislation. Like the more widely reported Cybersecurity Law (which went into effect on June 1).

> Article 28: Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law.[20]

This law requires companies which operate computer and telecommunications networks to assist the Chinese government in any number of activities so long as it is for law enforcement or national security purposes. This would include companies like Huawei and ZTE, and could force them to allow Chinese security and intelligence services into any network they operate around the world.

5G AND SMART CITIES

In recent years, every major U.S. telecommunication provider unveiled some form of operational 5G networks and compatible phones. More than one hundred operators have more than 4000 local network deployments in the United States and more than 7000 deployments globally according to Ookla, a company which specializes in telecommunication analytics. 5G promises download and upload speeds that far exceed that of the previous generation cellular networks (4G). So, what is 5G, and does it live up to all the hype?

5G is the most recent next-generation mobile phone network band which, in theory, will eventually replace or at least augment 4G networks. 5G genuinely brings faster speeds and drastically reduced latency, i.e., the time it takes data to travel from one point to another. Think about two semi-trucks each loaded with the exact same amount of cargo, only one is traveling at 65mph and the other is traveling at 250mph. Download and upload speeds could be akin to how fast the semi-truck gets unloaded and loaded.[21]

Unlike previous generations of mobile networks, 5G operates on three different spectrum bands: Low-band, Mid-band, and High-band. Each band tends to correspond to the level of performance provided by each one, low, medium, and high. Each band comes with its own advantages and drawbacks and the United States, European Union, and China are investing and employing networks in each band range.

Low-band: *Digital Trends* and *PC Magazine*, both separately and independently, found that the most widespread 5G networks available today perform better than the current 4G LTE standard, however not by much. Exact performance numbers were not available but looking at theoretical numbers, peak 4G speeds are around 100Megabits per second (Mbps) and peak 5G speeds in low-band are the same or very similar according to GSMA. The slight better performance of 5G is likely due to less demand placed on 5G networks. If each cell tower node can handle 100 Mbps, each user connected to that tower has to share that data rate so if 50 users are connected to each node, they are only going to get a maximum on 2 Mbps regardless of 5G or 4G coverage.[22]

As the mid-band continues to become more common place, low-band will less often be used for mobile broadband, and more often used for Internet-of-Things (IoT) sensors, self-driving cars, mobile medical devices (excluding remote surgery), and the like. Low-band is inherently more reliable due to the ability of its propagated signals to travel father distances, through denser-than-air mediums such as walls, flesh, and especially inclement weather where precipitation and clouds could affect the effective range of 5G signals. Low-band networks will operate between frequencies 5 Megahertz and 1 Gigahertz. The general rule-of-thumb is the lower the frequency, the farther a signal will travel and still retain enough energy over that distance to be 'heard' by the antenna in a cellphone.[23]

Mid-band: The "next step up" grants significantly better speeds and significantly shorter cell tower ranges. The science shows a peak data rate of up to 1 Gigabits per second which translates to blisteringly fast cellphone download speeds although real-world speeds may vary depending on environmental effects and Wide Area Network (WAN) data demand. That data rate is still shared by every user on the network however instead of the 2 Mbps in low-band, its 20 Mbps when divided among 50 users on the node. Mid-band will operate in the 1-6 GHz range with 3.5 GHz being the most common. This frequency falls

20. "Translation"; Tanner, "Beijing's New National Intelligence Law"; Bowman, Hou, and Li, "A Primer on China's New Cybersecurity Law"; People's Republic of China, "Translation." China's National Intelligence Law, enacted on June 27 with unusual speed and limited public discussion, is a uniquely troubling milestone in Beijing's four-year-old campaign to toughen its security legislation. Like the more widely reported Cybersecurity Law (which went into effect on June 1)

21. Qualcomm, "What Is 5G | Everything You Need to Know About 5G | 5G FAQ," Qualcomm, July 25, 2017, *https://www.qualcomm.com/invention/5g/what-is-5g*; Sascha Segan, "What Is 5G?," PCMAG, accessed April 23, 2022, *https://www.pcmag.com/news/what-is-5g*.

22. Segan, "What Is 5G?"; Christian de Looper, "5G Coverage Map: Cities with 5G on Verizon, AT&T, T-Mobile," Digital Trends, April 20, 2022, *https://www.digitaltrends.com/mobile/5g-availability-map/*.

23. Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017). (n.d.). Retrieved April 23, 2022, from http://newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

under C-Band radio waves, as regulated by the Federal Communications Commission and the International Telecommunications Union, (different from the L/M/H band discussed in this paper) which are also used for satellite communications.

To make mid-band work, most cities plan on installing multiple antennae in places like streetlamps, traffic lights, and other locations which are both plentiful, and powered on the city grid. This plan will mitigate the problem of having such a short signal range, however it will likely take many years for mid-band 5G to reach more remote areas like interstates and highways, small towns, and even homesteads/ranches.

There are also two techniques called "Massive MIMO" (Multiple Input Multiple Output) and beamforming which will help compensate for the propagation loss over distance. Massive MIMO essentially groups together antennae at the transmitter and receiver to provide better power usage efficiency, and more efficient use of the electromagnetic spectrum. Beamforming is a data traffic control system for mobile broadband networks that identifies the most efficient data-delivery route to a particular user and reduces interference for nearby users in the process.

High-band: These frequencies are extremely rare and fragmented globally. Only a handful of places around the world utilize this band, and even fewer cellphones are compatible. All of the frequencies in this range are above 6 GHz, with most high-bands in the 26-28 GHz range. And while the range of these signals are not great, usually covering only a single building or less, the data rate in real world environment could easily reach 10 Gbps of shared data.

Why It Matters

This paper is primarily concerned with the low-band as it is on those frequencies which smart cities currently operate and will continue to operate for the foreseeable future. 5G further enables IoT sensors and will likely have dedicated networks for IoT devices only, to prevent interference and reduce strain on the public and government network infrastructure. The added use of beamforming and Massive MIMO will further enhance the efficiency of such 5G networks and enable more IoT devices on any given network.

IOT DEVICES

As one may have surmised thus far, 5G IoT extends wireless internet, or at the very least, network connectivity to devices outside of the normal laptops, tablets, smartphones, and TVs. 'Dumb' devices which gain network connectivity become 'smart' and as such can communicate and be controlled remotely through a network connection. This serves to automate a variety of tasks as mentioned in the previous smart city section; essentially, IoT devices embedded in smart city infrastructure, or on smaller scales like homes, factories, hospitals, government buildings, etc., serve to drastically increase efficiency in all its forms. All of these buildings combined together, form a smart city.[24]

Smart homes are the smallest scale where these devices come to play. For example, an individual comes home, and the garage door automatically opens because the car communicated with the garage as he pulled into the driveway. The individual's biometric sensor implant indicates that the user has had a rough, stressful day. So, the house computer set lighting to a lower intensity and perhaps the user's chosen color for relaxation. The thermostat adjusts temperature automatically based on whether there are any occupants at home to conserve energy.

In a business, smart sensors may be in meeting rooms or a conference center. Smart systems will assist employees in locating and scheduling an available room for a meeting, ensure the proper room type, size and features are available for use. The meeting room temperature will adjust according to the occupancy level, and the lights will dim in anticipation of the PowerPoint presentation. Factories could benefit by installing smart sensors in assembly lines. Manufacturers outfitted with sensors will provide sensor data to the plant operator, informing them of anomalies and predicting when parts will need to be replaced thus preventing unexpected downtime which would result in less production and lower profits.[25]

In smart cities, IoT devices will be used in a seemingly endless number of ways to improve the quality of life of everyday citizens. Smart infrastructure is more energy efficient, increases performance of their

24. Frank Hamilton, "How Are IoT Based Devices Helping The Cities Grow Smarter," IoT For All (blog), January 1, 2020, *https://www.iotforall.com/smart-city-iot-applications*; Brien Posey, "What Are IoT Devices? - Definition from *TechTarget.Com*," IoT Agenda, accessed April 23, 2022, *https://www.techtarget.com/iotagenda/definition/IoT-device*.
25. Hamilton, "How Are IoT Based Devices Helping The Cities Grow Smarter"; Posey, "What Are IoT Devices?"

intended function, and helps cities become more environmentally friendly. LED streetlights that only light up when they sense movement, air pollution and emissions forecasts, optimize traffic flow by adjusting traffic lights to ease the flow, smart parking to show and even claim parking spaces using ones smart phone of in-car computer, even smart waste management by trashcans which indicate to trucks when they are full to create the most fuel efficient pickup schedule, are all ways which smart technology will help improve the quality of life in large, smart cities.[26]

HISTORICAL CHINESE SPYING STRATEGIES

As early as 1950. There have been documented cases of Chinese spying against the United States – usually – to steal state secrets, research, and often counter U.S. Foreign policy especially in areas where China deems a threat to their security from Western influence. In 1950, Qian Xuesen, a professor at Caltech and co-founder of the jet propulsion laboratory, was stripped of his security clearance for alleged connections to the CCP. Qian worked with former German rocket scientists following WWII and worked on the Manhattan Project. Following five years of house arrest, Qian is deported to China and later becomes the Father of Chinese Rocketry.

In 1979, the United States normalized relations with China, and within three years, roughly 10000 Chinese students were living in the United States. The FBI – from at least 1979 to presumably present-day – directed field offices to groom and specifically select valuable Chinese students for counterintelligence operations. [27]

Throughout the 1990s, economic espionage increased dramatically. So much so, that in 1996, Congress passed the Economic Espionage Act, which made it a federal crime to steal trade secrets on behalf of a foreign power or with the intent of causing harm to the company. [28]

The 2000-2010s were even more intense. Dongfan Chun was the first person to be convicted under the Espionage Act; for stealing classified documents on the B1 Bomber, F-15 fighter jet, Chinook helicopter, and the U.S. Space Program while working for Boeing and Rockwell, earning millions of dollars as compensation. From 2010-2012, China executed over 20 people who were convicted by Chinese authorities of being spies for the United States. In 2014, the U.S. Department of Justice indicted a Chinese military hacking group known as "61398" who were found to be hacking into U.S. Companies, stealing intellectual property, business plans, negotiation strategies, and other items for the benefit of Chinese companies. [29]

Most relevant to this paper, in 2014, T-Mobile filed a lawsuit against Huawei, citing stolen software and hardware by Huawei employees. Later in 2019, the U.S. Department of Justice charged Huawei with purposefully stealing trade secrets from T-Mobile. [30]

To be clear, this list is not exhaustive. This section seeks merely to highlight the evolution of Chinese intelligence collection tradecraft over time and their increasing reliance on technical collection means. China has often focused on stealing intellectual property and other economic-related information, likely to catch-up with other developed countries in terms of technology and military capability.

RECENT CHINESE SPYING DEVELOPMENTS

In May 2019, the United States government began the legal process to formally outlaw US Companies from conducting any business with the Chinese tech giant Huawei as well as ZTE and further restricted their ability to conduct any sales within the United States or its territories. Former President Donald Trump signed an executive order on May 15, 2019, declaring a national emergency, which placed Huawei and ZTE on a list designating them as national security risks. The Department of Commerce then placed the firms on an "entity list" which requires US firms to seek government permission before doing business with Huawei. After federal court proceedings, Huawei was officially banned in the United States in 2021.[31]

Other major tech companies around the world, some of which are not owned or based in the U.S.,

26. Ibid.
27. Alexander Holt, "A Brief History of US-China Espionage Entanglements," MIT Technology Review, accessed April 19, 2022, *https://www.technologyreview.com/2020/09/03/1007609/trade-secrets-china-us-espionage-timeline/*.
28. Holt.
29. Holt.
30. Holt.
31. Haridy, "Huawei, the US Ban, and Links to Chinese Spying Explained"; Porter, "US Delays Full Huawei Ban yet Again until May 15th"; Emily Feng and Amy Cheng, "China's Tech Giant Huawei Spans Much Of The Globe Despite U.S. Efforts To Ban It," NPR, October 24, 2019, sec. World, *https://www.npr.org/2019/10/24/759902041/chinas-tech-giant-huawei-spans-much-of-the-globe-despite-u-s-efforts-to-ban-it*.

also cut their ties, deciding to stay in the good graces of the United States over China. Huawei relies on heavily American companies like Google's Android Smartphone OS "Snapdragon," Microsoft's computer OS "Windows 10," and the computer chips made by Qualcomm and Intel as well, for the vast majority of their manufactured devices. Even companies like Vodafone, Arm, and EE all shelved plans to sign new deals with Huawei, including the launch of Huawei's new 5G phones (which will no longer be receiving OS updates from Google's Android).

These new restrictions revolve around China and Huawei's, at minimum, lack of concern for U.S. intellectual property. Chinese companies like Huawei and ZTE that either directly or indirectly cooperate with various elements of the Chinese government, and suspicious instances where Chinese commercially sold networking products were breached. Statistically, Chinese products carry the highest instances of security flaws when compared to American, Korean, and Japanese products.

Huawei: Huawei is the world's largest single telecommunications equipment provider. Not only does it make cell phones and other connected devices, but it also makes every component for network infrastructure of the emerging 5G networks. U.S. Lawmakers were successful in preventing Huawei tech from being used in American network infrastructure, instead opting for American and South Korean companies like Cisco, Microsoft, Qualcomm, and Samsung.[32] Some other countries did not opt out of Huawei's equipment, including some strong U.S. allies. All parties of the FVEY agreement (Five-Eyes: U.S. Canada, United Kingdom, Australia, and New Zealand; an anglophone intelligence sharing alliance; all parties to the AUG 14, 1941, UK/US agreement) have at least limited Huawei equipment to varying extents.

While there is little quantity of open-source hard evidence alleging backdoors are built into Huawei's equipment what does exist carries significant weight. Recently, U.S. Officials confirmed that Huawei can access those networks it helped build that are being used by mobile phones around the world. Huawei has reportedly been using backdoors intended for law enforcement by the domestic Chinese government for well-over a decade according to The Wall Street Journal and CNET, citing US officials. The details were disclosed to the United Kingdom and Germany at the end of 2019 after the US had noticed access since 2009 across Chinese 4G equipment.

The backdoors were allegedly inserted for law enforcement use into carrier equipment like base stations, antennae and switching gear with US officials alleging they were designed to be accessible by Huawei. However, cyber security experts say there doesn't need to be any hard evidence if Huawei cooperates either willingly with, or through coercion by the Chinese government. "We have evidence that Huawei has the capability secretly to access sensitive and personal information in systems it maintains and sells around the world," Robert O'Brien, National Security Adviser, reportedly said.

Huawei needs to be able to send out software updates the same way Google, Apple, and Microsoft do so as well. Assessment: if Huawei were directly cooperating with the CCP, they could send out malware disguised as a software update thus allowing whoever owns the malware to presumably access information on the device or network component. If a link from Huawei's China headquarters to cell towers in the U.S. were made, it would likely present a "strong risk" of Chinese intelligence services using it to sneak malware into U.S. communications networks. In fact, as will be discussed in detail later in this paper, Chinese companies are legally required to cooperate with government investigations of any kind which could include handing over information stored on or passing through their hardware.

This could essentially compromise every piece of data flowing through the network, from phone calls and text messages, to browsing history, financial and banking information, and other PII. On a 5G network within a smart city, this places at risk vital city functions like standard utilities (energy, water, etc.), traffic cameras, and various e-governance systems. If "country X" with Huawei's smart city tech had a confrontation with the Chinese government, ransomware for example, could be used to help coerce cooperation on an issue.

Evidence also exists of Huawei breaking international law by violating U.S. Sanctions on Iran. This revelation reduces the company's overall trustworthiness and shows the lengths at which Huawei is willing to go to make a profit. According to a timeline provided by CNET, documents were leaked on March 2, 2020, that revealed Huawei's roles in shipping prohibited U.S. Technology to Iran. In January 2019, US federal prosecutors placed 23 indictments on Meng Wanzhou, Huawei's chief financial officer, and her employer, Huawei, for a variety of alleged crimes, including bank and wire fraud, conspiracy to defraud the US, and stealing trade secrets (a Chinese hallmark). Wanzhou

32. Ibid.

was arrested by Canadian authorities at the request of the U.S. Department of Justice in December 2018.[33]

The Intelligence Community has warned about close ties between the CCP and Huawei executives for years and further banned Huawei from competing for U.S. government contracts in 2012. Huawei mistrust has historically stemmed from the fact that the company's founder and current CEO, Ren Zhengfei, was a research and development specialist in IT and telecommunications for the People's Liberation Army prior to founding the now tech giant.[34] Perhaps more importantly, the Chinese government has invested tens of billions of dollars in the company as well as provided numerous subsidies to support its international growth. Fears have only been worsened after China's passage of its National Intelligence Law and cybersecurity laws in 2017, which, according to Bloomberg's Eli Lake, "compel corporations to assist in offensive intelligence operations" instead of just requiring them to cooperate with law enforcement on national security matters, thus implicating the companies as branches of the Chinese intelligence collection apparatus.[35]

ZTE and Lenovo: These companies have very similar issues to those described in the Huawei section. They are still beholden to the 2017 National Intelligence Law and other cyber security laws as well. However, they are smaller companies who do not pose as great a threat due to their smaller global footprint. ZTE is subject to the same economic restrictions as Huawei as they are also a 5G telecommunications provider, cellphone manufacturer, and maintain close ties with the Chinese Communist Party. The 2012 House Intelligence Committee report on Huawei and ZTE, found that neither Huawei nor ZTE "fully cooperate[d] with the investigation and [were] unwilling to explain [their] relationship with the Chinese government or Chinese Communist Party." The report concluded that the US "should view with suspicion, the continued penetration of the US telecommunications market by Chinese telecommunications companies."[36]

Lenovo has had numerous, serious security flaws built into its products throughout the last few years. The Lenovo Service Engine for example, was installed on devices from 2014 to 2015. It was designed, according to *MakeUseOf.com* website – whose "mission is to help users understand and navigate modern trends in consumer technology" – to supposedly send non-identifiable system information from the PC to Lenovo, the first time the computer goes online. It seems fairly innocent, however, that Lenovo Service Engine had various security issues, and as a result, could allow hackers to gain access to the PC.[37]

Furthermore in 2014, Lenovo laptops shipped to stores and consumers that had malware preinstalled but was disguised as a piece of typical manufacturer bloatware ('useful' software to some, they are programs that come preinstalled on a brand-new computer and are very difficult to remove for the average consumer). Superfish Visual Discovery was a browser extension that analyzed images, checked to see if they were products, and then displayed cheaper alternatives.[38]

However, Superfish essentially was a hacking tool that hijacked browsers. The program worked by installing a self-signed HTTPS certificate, which makes HTTPS connections as weak as HTTP. In layman's terms, it enabled Superfish to intercept internet traffic which is known as a Man-in-the-Middle attack,

33. Keane, "Huawei Ban Timeline"; U.S. Dept. of Justice, "Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged With Financial Fraud," January 28, 2019, *https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged-financial*.

34. Huawei Ltd., "Mr. Ren Zhengfei - Huawei Executives"; Brendan Pierson and Karen Freifeld, "By Spying on Huawei, U.S. Found Evidence against the Chinese Firm," Reuters, April 4, 2019, sec. Banks, *https://www.reuters.com/article/us-usa-china-huawei-tech-idUSKCN1RG29T*. U.S. authorities gathered information about Huawei Technologies Co Ltd through secret surveillance that they plan to use in a case accusing the Chinese telecom equipment maker of sanctions-busting and bank fraud, prosecutors said on Thursday.

35. Hal Brands, "Huawei's Decline Shows Why China Will Struggle to Dominate," *Bloomberg.Com*, September 19, 2021, *https://www.bloomberg.com/opinion/articles/2021-09-19/huawei-s-decline-shows-why-china-will-struggle-to-dominate*; Jordan Robertson and Jamie Tarabay, "Chinese Spies Accused of Using Huawei in Secret Australian Telecom Hack - Bloomberg," accessed April 13, 2022, *https://www.bloomberg.com/news/articles/2021-12-16/chinese-spies-accused-of-using-huawei-in-secret-australian-telecom-hack*.

36. Anita George, "Your Lenovo Laptop May Have a Serious Security Flaw," Digital Trends, August 26, 2019, *https://www.digitaltrends.com/computing/lenovo-laptops-security-flaw/*; Bill Gertz, "Lexmark, Lenovo Tech Funnels Data to China Intelligence Services," The Washington Times, accessed April 23, 2022, *https://www.washingtontimes.com/news/2020/feb/24/lexmark-lenovo-tech-funnels-data-china-intelligenc/*. A newly discovered security vulnerability involves older Lenovo laptops and a no-longer-supported program called Lenovo Solution Center. The laptop manufacturer has advised customers with these laptops to go ahead and uninstall Lenovo Solution Center to protect their computers." Leading Chinese technology companies have sold equipment to state governments in the U.S. that can be used by Beijing to obtain sensitive information, according to a security analysis made public Monday.

37. George, "Your Lenovo Laptop May Have a Serious Security Flaw"; Christian Cawley, "Why You Should Avoid Lenovo PCs: 7 Security Risks to Consider," MUO, May 13, 2016, *https://www.makeuseof.com/tag/security-failings-demonstrate-avoid-lenovo/*; Gertz, "Lexmark, Lenovo Tech Funnels Data to China Intelligence Services." Think your Lenovo laptop is safe and secure? Think again! Various security risks and vulnerabilities have plagued Lenovo PCs. Leading Chinese technology companies have sold equipment to state governments in the U.S. that can be used by Beijing to obtain sensitive information, according to a security analysis made public Monday.

38. George, "Your Lenovo Laptop May Have a Serious Security Flaw"; Cawley, "Why You Should Avoid Lenovo PCs"; Gertz, "Lexmark, Lenovo Tech Funnels Data to China Intelligence Services."

one of the most common cyberattacks in online crime. These self-signed HTTPS certificates had the same private encryption key on every single affected Lenovo computer made from 2014 to 2015 but has since been discontinued.[39]

The latest known Lenovo security issue came from the Lenovo Solution Center (LSC) in May 2016. The LSC was yet another piece of bloatware that introduced a vulnerability to one's home network. It included a privilege escalation vulnerability that allowed attackers with access to a device on one's personal network to execute malicious code. While home networks are generally secure, public Wi-Fi is not. The attacker need only connect to the same network as the target device and after a few keystrokes, could compromise the device utilizing the privilege escalation vulnerability. Later, when the device was brought home and connected to the home network, it too became compromised. LSC was installed on all Lenovo devices until November 2018.[40]

These issues do not necessarily implicate Lenovo in some greater Chinese intelligence collection program as is likely the case with Huawei and ZTE. But these issues were enough to prohibit the use of Lenovo computers on government networks and prevent them from competing for government contracts. Lenovo also has a quickly growing server manufacturing business as well which could be a future threat. As it stands at the time of this writing, Lenovo is not subject to the Department of Commerce's list of companies who pose national security risks. That does not, however, exonerate them as they are still beholden to Chinese cyber and intelligence laws.

TikTok: According to Business Insider, TikTok has over 1 billion monthly active users. The app's concept is to let users easily share short video clips that can get a lot of views very quickly. There are numerous issues with the app concerning child safety from potential predators and censorship of content that may run contrary to CCP rhetoric (TikTok has stated that it handles censorship differently by region).[41]

However, there are definite privacy issues as well. Upon the close examination of the apps permissions when attempting to download it (the author did not), one would find the following permissions granted: take pictures and video, read contacts, record audio, modify, or delete the contents of one's shared storage, and read the contents of shared storage. All of that seems necessary for the app to function. Then there is the "Other Permissions" category, akin to the 'fine print' of any contract or terms and conditions. Permissions like "have full network access," "run at startup," and "retrieve running apps" could all give the app some undue access into one's device. New updates pose the most serious risk as they "may automatically add additional capabilities" potentially without asking permission of the device's owner/user.[42]

TikTok is a recent Chinese acquisition of the former American company "*musical.ly*." The concerns over TikTok center on cybersecurity and spying by the Chinese government. There is a national security review dedicated to assessing the threat presented by TikTok, and it is ongoing, but there are some key facts that are open-source. The app has the capability to convey location, image, and biometric data (facial recognition) to its Chinese parent company, which is legally unable to refuse to share data to the Chinese government.[43]

The DoD put out an advisory memo which states "TikTok (formerly *Musical.ly*) application 12.2.0 for Android and iOS performs unencrypted transmission of images, videos, and likes. This allows an attacker to extract private sensitive information by sniffing network traffic." Furthermore, independent Check Point Research released a report that detailed multiple vulnerabilities in the TikTok app that would allow attackers to compromise accounts, obtain otherwise secure data, modify/delete/write device storage, and reveal personal information saved on the account. Check Point is a security research firm that has discovered vulnerabilities in other apps used daily and has a track record of working with developers to make them aware of issues to be fixed. This latest revelation, however, simply highlights the growing problem presented by Chinese software.[44]

39. Ibid.
40. Ibid.
41. Jason Aten, "The Department of Defense Is Warning People Not to Use TikTok Over National Security Concerns," *Inc.com*, January 9, 2020, *https://www.inc.com/jason-aten/the-department-of-defense-is-warning-people-not-to-use-tiktok-over-national-security-concerns.html*; Shona Ghosh Morgan Clancy, "What's Going on with TikTok?," Business Insider, accessed April 23, 2022, *https://www.businessinsider.com/whats-going-on-with-tiktok-censorship-privacy-2019-11*; Neil Vigdor, "U.S. Military Branches Block Access to TikTok App Amid Pentagon Warning," *The New York Times*, January 4, 2020, sec. U.S., *https://www.nytimes.com/2020/01/04/us/tiktok-pentagon-military-ban.html*.
42. Aten, "The Department of Defense Is Warning People Not to Use TikTok Over National Security Concerns"; Morgan, "What's Going on with TikTok?"; Vigdor, "U.S. Military Branches Block Access to TikTok App Amid Pentagon Warning."
43. Ibid.
44. Ibid.

METHODOLOGY

Research Method Approach

Quantitative and qualitative research are both utilized in this paper, however qualitative research is the most prolific, in the form of narrative analysis and content analysis. The narrative analysis will focus on case studies that will frame the problem and provide context for the threats presented by the proliferation of technology made, designed, and maintained by Chinese companies. Content analysis will derive meaning from raw data such as maps and charts detailing Chinese investment in foreign network infrastructure and the relationships of concepts between them; it will allow the preponderance of conclusions from that data. Content analysis will also help mitigate bias, as certain themes, word, or concepts could be indicative of a political slant or some other agenda. Quantitative data is minimal but could still provide greater support to the analysis; for example, the sheer number of countries within which China invests in network infrastructure. The clustering of countries could correlate with a regional focus for China at the global strategic level in Africa and South-Central Asia, for instance.

This paper utilized over 100 online secondary sources, including a source (Congressman Gallagher; WI) who summed up many of the national security threats presented by Huawei/ZTE, 5G networks, and smart cities within the scope of Chinese Communist Party influence. Not every source was directly used in the synthetization of this paper, instead being utilized as additional support towards key claims. When multiple sources make the same or very similar claims and convey the same facts, it reduces the chances of relaying false or misleading information through this paper. Every claim made through this paper can either be verified through at least two sources or is a product of the author's analysis and experience within the world of military, intelligence, and counterintelligence. No claims or analysis by the author of this paper was made with the aid of privileged information whatsoever.

Types of Sources

All the sources for this paper are secondary sources. All the information is from reputable and noteworthy sources, or sources with which the author has had positive interactions within previous research. 'Western' government organizations where the host countries have press and speech freedoms as well as a reasonable degree of transparency are highly sought out/emphasized for this paper because they tend to provide the most accurate, unbiased, and relevant information to intelligence topics like this. Western NGOs and trade journals with the same legal protections are also very important types of sources, and they may also report on information that governments do not publish or confirm/deny knowledge of for security reasons. Last, newspaper articles can be useful, especially when seeking out the origins of information (the original source that the journalist used). However, news outlets are typically the most susceptible to bias, false reporting, and other types of inaccuracies due to the agendas of their corporate leadership, as well as a general lack of analytic rigor and proper assessment of potential threats (a tendency to catastrophize events and draw conclusions based on limited data).

Bias Mitigation

Structured analytic techniques such as those described in "Structured Analytic Techniques for Intelligence Analysis" by Randolph Pherson and Richards Heuer Jr. are the primary bias mitigation method. Methods like "Key Assumptions Check" and "Indicator Generation, Validation, and Evaluation" will help assess the validity of information and keep research on the right path towards answering the initial questions. A large variety of sources will also help this paper grasp the entirety of the problems from different angles and perspectives; as well as corroborate claims.

COLLECTION METHODS AND TOOLS

Methods

The entirety of the research conducted, was via the internet. It is unlikely that other mediums have much published on the topic of Chinese tech companies and the CBRI that isn't already on the internet first. Since this topic primarily concerns current events and is constantly evolving, physical printed books do not hold much value for this topic. Anything that is printed in a book is probably already on the internet is some form or another. If this were a historical research paper, this would not be the case.

Tools

Google Scholar, Incognito Mode, etc.: Google is obviously the preeminent search engine for most of the world. Boolean logic searches can help find the best and most relevant sources.

TOR Browser; for confidential research as well as finding different news sources based on the IP address of the user. Easy secure VPN setup as well.

STRUCTURED ANALYTIC TECHNIQUES FOR INTELLIGENCE ANALYSIS

Analytic Design
Identify Patterns and Indicators

Identifying patterns and indicators is essential to answering the research questions for this paper. This paper is structured closer to a court case than it is to a testable hypothesis. All the evidence must be examined, to establish the likelihood and confidence level of the answer to the research question. For example, "this paper believes with (very high/high/moderate) confidence that the Chinese government is doing X, Y, or Z, as evidenced by exhibits 1, 2,... and 6. It is furthermore (very likely/likely/reasonable to assume) that the Chinese government has the intent to conduct X, Y, or Z against the United States or its interests as evidenced by China's historical conduct in this arena." Patterns, indicators, and simple pieces of evidence are what will best support this style of research and question answering. It is difficult to hypothesize on this topic, as it is multifaceted.

Limitations

This research as some limitations that limit the ability of this paper to truly answer the research questions beyond any reasonable doubt. The biggest one is the available data. This paper relies entirely on publicly available information, and the author does not seek out, nor does it employ the use of any privileged information even if it could shed light on some information gaps. Furthermore, the author lacks technological expertise, he is not a software/computer/electrical engineer or a Certified Ethical Hacker. The author analyzes capabilities but has limited capacity to do any hands-on research such as penetration testing or ethical hacking on Chinese equipment.

This paper also utilizes certain case studies where Chinese network and telecommunications equipment was at fault for, or involved in, a compromise of some kind. However, case studies only give preponderance of the evidence, not beyond reasonable doubt in legal terms. Therefore, other aspects such as the historical use of espionage, their Tactics, Techniques and Procedures (TTPs), and their assessed grand strategy must also be analyzed.

ANALYSIS AND DISCUSSION

The analysis of this paper, centers on case studies. The case studies are designed to explain the 5W+Hs (Who, What, When, Where, Why, + How) to the reader as a piece of evidence – an indicator – that contributes to the solving greater ambiguity surrounding Huawei, China, and like topics. The combination of multiple case studies with similar circumstances can establish patterns of behavior, trends, and a baseline/precedent for escalation. The first set of case studies does not directly relate to the compromise of Huawei and other Chinese devices. Instead, it establishes a pattern of behavior indicating a willingness to skirt well-established laws, regulations, and guidelines when from Huawei's perspective, the potential gain outweighs the risk or the cost. The second set of cases directly concerns the compromise of Huawei, most likely by Chinese intelligence entities. There are limited numbers of case studies available due to an overall lack of credible reporting and sources.

CASE STUDIES: PART ONE – A PATTERN OF ILLEGAL BEHAVIOR

Government Financial Support and Industrial/Economic Espionage

Huawei receives significant and continuing financial support from the Chinese government in the form of subsidies, tax breaks, and research grants. This financial advantage combined with highly likely instances of economic espionage make it exceedingly difficult for other companies to compete with Huawei. Huawei is one of the few companies that offer a one-stop-shop for countries seeking to upgrade their telecommunications networks to 4 & 5G. The Chinese

Belt and Road Initiative (CBRI) makes this technology more accessible, even to poorer developing nations by offering loans with predatory terms. Huawei offers the same – in some cases, literally the same – technology for a significant discount in comparison to their competitors as a result of the financial assistance from the Chinese government.

Specifically with regard to economic espionage, there are numerous cases from which a Chinese company or the Chinese intelligence services conducted spying operations. Cisco, an American company, for example accused Huawei of replicating some of their commercial products, including the design flaws and manual typos. Motorola stated that Huawei successfully recruited some of its employees to steal intellectual properties and product designs. As described later in this paper, a Huawei executive was used to recruit a cybersecurity expert as a spy in Poland's Foreign Intelligence Agency. Huawei incentivizes their employees to steal "valuable information" from competitors via a company program for their Chinese employees according to lawsuit court documents.[45]

Bypassing Sanctions and Bank Fraud

In 2019, following a FISA warrant search, evidence was found against Huawei and the Huawei CFO, Meng Wanzhou (daughter of the company's founder Ren Zhengfei), that could prove guilt in conspiring to defraud HSBC Holdings Plc and several other banks, and in operating a front company to avoid sanctions on Iran, as well as 11 other lesser charges. Meng Wanzhou was eventually released, however the charges against the company remain in place. While Huawei asserts that the suspected front company "Skycom Tech Co Ltd" was simply a business partner, the U.S. Federal prosecutor's indictment said that it is a front company designed to conceal business deals with Iran. Huawei is accused of using Skycom to move embargoed goods and tech services, including U.S. technology such as Hewlett-Packard computers, into Iran. An internal HSBC probe led to additional charges against Huawei and Meng revealing the bank and wire fraud by moving U.S. Dollars into and out of Iran thus misrepresenting the relationship with a company doing illegal business in Iran.

The same indictment also charges Huawei with doing business in North Korea, which is a violation of not only the U.S. sanctions, but the E.U. and U.N. restrictions as well. Huawei is suspected of helping North Korea maintain and build their telecommunications networks. The restrictions are designed to degrade North Korea's ability to conduct nuclear and weapons research as well as punishment for human rights abuses.

This intelligence obtained from the FISA warrant was collected from Chinese telecom executives as they passed through American airports from their electronic devices (according to Reuters). These allegations – if true – could shed light on the lengths at which Huawei is willing to break U.S. and international law; as well as highlight how the Chinese government refuses to hold their domestic companies and persons accountable for their actions. If Huawei can conduct this type of activity without any consequence, it is not too difficult to believe that Huawei, as an all-encompassing entity for their subsidiaries, is also probably willing to use its technology as a backdoor to gain information for their own advantage from competitor companies – with or without input or direction from the Chinese government or the CCP.[46]

Huawei Executive as a Cover Identity for a Suspected Spy

In January of 2019, Polish authorities arrested two individuals for spying on behalf of China. One individual was a former Polish secret services agent for their "Foreign Intelligence Agency" – the Polish synonym for the American CIA. The other was a Huawei executive who also worked for the Chinese intelligence service and recruited the Polish intelligence officer and cyber security expert as a spy. Polish court documents indicate that the Huawei executive was using illegal means – including espionage – to influence the future of Poland's telecommunications infrastructure for at least the last seven years. The Polish intelligence officer used his access "at the top levels of government" to inform the Huawei executive about Polish rescue and safety services radio networks; the same networks used by their emergency services and law enforcement agencies. Huawei fired the executive after his arrest by

45. Annie Fixler and Mikhael Smits, "Huawei Endangers Western Values"; Pierson and Freifeld, "By Spying on Huawei, U.S. Found Evidence against the Chinese Firm"; Vincent Ni, "Documents Link Huawei to Uyghur Surveillance Projects, Report Claims," The Guardian, December 15, 2021, sec. Technology, *https://www.theguardian.com/technology/2021/dec/15/documents-link-huawei-uyghur-surveillance-projects-report-claims*; Chris Burns, "US Huawei Phone Spying: Here's The Incentive," *SlashGear.com*, January 29, 2019, *https://www.slashgear.com/us-huawei-phone-spying-heres-the-incentive-29563952/*

46. Keane, "Huawei Ban Timeline"; U.S. Dept. of Justice, "Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged With Financial Fraud"; Pierson and Freifeld, "By Spying on Huawei, U.S. Found Evidence against the Chinese Firm"; Burns, "US Huawei Phone Spying."

Polish counterintelligence services but has continued to fund his legal fees.

This case is another indication that Huawei frequently breaks the rules in search of an advantage in their business dealings. Since it is also likely that Huawei targeted law enforcement communications through more traditional human intelligence sources and tradecraft, it could indicate greater involvement by the Chinese government in securing economic advantage on behalf of Chinese government; the Huawei executive had to have received espionage training from some entity with the tradecraft knowledge and expertise. China could easily use Huawei tech as a backdoor into Polish law enforcement official communications channels where they could wiretap or even shut down this network and hold it hostage during a time of crisis and to force capitulations.

It is furthermore unclear what economic value that the information passing through law enforcement channels has. It is far more likely that that sort of information would be more useful to the Chinese intelligence services rather than to Huawei. The simple fact that a Polish intelligence officer with cybersecurity expertise may have been targeted, groomed, and recruited as a spy, by a person who may have been a Chinese case officer masquerading as a Huawei executive, indicates potentially greater involvement from Chinese intelligence services.[47]

CASE STUDIES: PART TWO – TECHNOLOGY SPECIFIC INSTANCES OF UNETHICAL & ILLEGAL BEHAVIOR

Chinese Citizen Loyalty Score

In a speech, former U.S. Vice President Mike Pence described it as "an Orwellian system premised on controlling virtually every facet of human life." However, according to Foreign Policy (FP), the system is not quite what it is hyped up to be – yet. [46] While there is a push in the CCP to develop such a system that operates throughout the entire country, the infrastructure isn't quite there just yet according to open sources, but they are getting closer. The system that is currently in place collects a vast amount of information on its citizens, more commonly known as big data.

One example of how China's social credit system is being used is that ran by Sesame Credit, a subsidiary of Alibaba – an online shopping store similar to Amazon or eBay. Unlike financial credit systems in western countries, Sesame takes both financial and social 'indicators of trustworthiness,' into account; all of it from big data mediums like social media and public/government databases. The system was created to remedy issues of trustworthiness by establishing a credit system. As recently as 2011 according to Time Magazine, only a third of Chinese citizens had a bank account, which meant most financial transactions were conducted in cash. With no system to show a credit report in place, people could default on loans, sell counterfeit goods, or have massive amounts of debt and the lender would never know until it was too late.

China is using elements of big data, artificial intelligence, and facial/gait recognition, as well as other forms of biometric identifiers to develop a profile for each and every individual citizen; and this could be broadened to include a profile on citizens of other countries as well if the Chinese were able to compromise smart city networks. All these steps will one day support its "social credit system" noted by Hon. Former Vice President Mike Pence. This and other developments being made both internally and overseas raise many serious concerns. Although the stated purpose of the system is to improve governance and market order by combating fraud and counterfeiting, the system could easily be used for other purposes such as counterespionage, putting down public protests by targeting group leaders, spying on foreign diplomats, and any number of other activities aimed at advancing their domestic and foreign policy interests. Huawei (and other Chinese companies), as China's leading tech company, is developing much of the infrastructure and software for this big data system.[48]

47. Pierson and Freifeld, "By Spying on Huawei, U.S. Found Evidence against the Chinese Firm"; Alicja Ptak and Justyna Pawlak, "Polish Trial Begins in Huawei-Linked China Espionage Case," Reuters, June 1, 2021, sec. China, *https://www.reuters.com/world/china/polish-trial-begins-huawei-linked-china-espionage-case-2021-05-31/*.

48. Annie Fixler and Mikhael Smits, "Huawei Endangers Western Values"; Colin Lecher, "Is Huawei a Security Threat? Seven Experts Weigh In," The Verge, March 17, 2019, *https://www.theverge.com/2019/3/17/18264283/huawei-security-threat-experts-china-spying-5g*; Katie Canales, "China's 'social Credit' System Ranks Citizens and Punishes Them with Throttled Internet Speeds and Flight Bans If the Communist Party Deems Them Untrustworthy," Business Insider, accessed April 23, 2022, *https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4*.

Huawei Facial Recognition Tech and Human Rights

Facial Recognition Software (FRS) is a relatively new technology – one that is still in its infancy as a general rule. It is software designed to use physical attributes of one's face to confirm their identity, similar to a fingerprint or DNA, though much less accurate. A variety of factors contribute to the accuracy of FRS, not least of which is the resolution of the image/camera. Other factors like atmospheric conditions (fog or humidity for example), lighting, camera angle, image orientation, and other conditions all have limiting effects on FRS. In the era of COVID-19 mask wearing, FRS is essentially useless in its current evolutionary state because the software is unable to discern features under a mask.

Various Chinese companies are developing FRS for the Chinese government and as commercial sales offerings. Most frequently, these FR systems are found in ports of entry and border crossings like road checkpoints and airports, as well as probably within and outside of some secure buildings as a security measure. China is very interested in these systems because they believe that it could be used to undermine political/social resistance groups by identifying group leaders, as well as identifying foreign spies, known or suspected terrorists, and the like.

Since at least 2018, Huawei and a Chinese AI company, Megvii, have been developing highly advanced Facial Recognition Software designed to detect certain people or groups based on operator input. As part of a system test for the compatibility of Huawei and Megvii software and components, the two companies trialed a feature called the "Uighur Alert." Another feature of the software is designed to determine the ethnicity of a target. The Uighur Alert could easily be used to flag a member of the highly oppressed minority group to authorities. Huawei and Megvii did not deny the document, recovered by IPVM (video surveillance analysis organization that discovered this revelation), they instead stated that it was only a test and has not been implemented in the "real world." Despite this, China has long been suspected of using technical surveillance to oppress various minority groups on the basis of race, religion, national origin, and especially political ideology.

The existence of this partnership between Huawei and Megvii resulting in the FRS brainchild is still a potential threat to U.S. interests and national security, regardless of whether the system has seen real-world application. This FRS – if implemented – could be used to track and reconnoiter targets of interest to the Chinese, such as political opposition group leaders, religious leaders, foreign spies, and plenty of others. If Chinese intelligence services were able to implement this system abroad – presumably on Huawei tech – then it could provide a wealth of facial recognition data by surveilling targets outside their own borders.[49]

African Union HQ Breach

Trade is growing roughly 20% with each passing year between Africa and China, and according to the BBC, China is Africa's largest trading partner. The increase in Chinese involvement, specifically investment, probably means that China increasingly desires to protect its investment. Part of a way to do so, is through the collection of intelligence. Intelligence can help the Chinese policy makers make educated decisions in their dealings across the entirety of the African continent through involving themselves in the African Union.

The African Union (AU) headquarters (HQ) building was completed in 2012 in the Ethiopian capital city, Addis Ababa. Greetings in Mandarin play through speakers when one enters the elevators, and fake palm trees bear the logos of the China Development Bank. The China Development Banks is a financial institution dedicated to advancing Chinese foreign policy under the direct leadership of their State Council (CCP). [12] China invested the entire $200 million price tag to build the AU's new HQ and it included a state-of-the-art computer server system.

This event was first reported by the French news agency "Le Monde Afrique" and independently verified and reported on by Financial Times a few days later. The AU's computer system had been gravely compromised. Both Le Monde and FT cited multiple "internal sources" which said from January 28, 2012 to sometime in late 2017, every night between midnight and 2AM, data was allegedly transferred to servers in Shanghai. It came to light in 2017, when an IT professional working for the AU recorded an unusually high amount of computer activity, which nearly maxed out data transmit capacity, on its servers during hours when the offices would have been deserted.

Upon this revelation, independent professional security teams swept through the entire building.

49. Pierson and Freifeld, "By Spying on Huawei, U.S. Found Evidence against the Chinese Firm"; Ni, "Documents Link Huawei to Uyghur Surveillance Projects, Report Claims"; Huawei Ltd., "Intelligent Video & Data Analytics," Huawei Enterprise, accessed April 13, 2022, *https://e.huawei.com/en/products/intelligent-vision*.

The teams reportedly found that microphones and other listening devices had been discovered in the walls and desks of critical and sensitive areas within the building. "This doesn't mean the company was complicit in any theft of data," said Danielle Cave from the Australian Strategic Policy Institute. "But... it's hard to see how - given Huawei's role in providing equipment and key ICT services to the AU building and specifically to the AU's data center - the company could have remained completely unaware of the apparent theft of large amounts of data, every day, for five years." There is no open-source smoking gun unfortunately that would confirm both the intent of China or its affiliates to hack the servers, and a deliberately placed vulnerability (backdoor).

Backdoors are not normal security vulnerabilities. Backdoors are intentionally placed and do not just require the existence of a security flaw or exploitable vulnerability. They also require 'hostile' intent. The hostile intent implies that the exploit (some flaw in the security coding) exists in the system because the hostile entity put it there on purpose. A Foreign Intelligence Entity (FIE) for example, may intentionally place the vulnerability within the system so that they can later return at will, and bypass normal authorization requirements such as passwords and other credentials for accessing the network. The vulnerability implies that the actor, first, is aware of the security flaw, and second, has the capability to exploit it. What is not publicly known, based on reputable facts, is the hostile responsible party – China, Huawei, or some other FIE – which would incriminate them in the AU hack.

Publicly, Both AU and Chinese officials branded the report as false and as an attempt by the West to damage relations between a "more assertive China and an increasingly independent Africa." However, Le Monde Afrique and FT said that AU officials had privately expressed concerns about their level of dependency on Chinese aid and how in theory, the Chinese could come to collect on the many favors (loans) they had done for the AU at any time.[50]

Huawei Malicious Software Update

China probably seeks to collect intelligence not just on the United States, but also on regional competitors like Australia, Japan, and South Korea – who also happen to be close U.S. allies. The priority level for the types of information sought by China is unclear, however they do have a documented history of targeting economic and technical information.

In 2012, Australian intelligence identified a very sophisticated intrusion into the country's telecommunications networks from a software update for one of Australia's largest telecom companies sent out from Huawei. The update contained malicious code that allowed access to these networks and worked very much like a wiretap. The code recorded all of the communications data sent over the network before deleting itself – a very sophisticated self-destruct feature. The breach was subsequently confirmed by other intelligence agencies within the FVEYs and by former intelligence officials who received briefings on the event. This incident has substantiated claims and suspicions from the U.S. government that China actively uses Huawei equipment as a spying conduit.

As a result of the intelligence sharing agreements between the United States and Australia, the USIC identified a similar cyber-espionage attack from China using Huawei equipment that was installed before it's ban in the U.S. National bans around the world have been in-part driven by this evidence that Chinese intelligence services – at the very least, if not with full cooperation from Huawei – exploit Huawei's products through manipulated software updates.

There is little evidence that Huawei had direct knowledge of, or intentional wrongdoing in the attacks at the higher levels within the company. The issue writ-large with Huawei is that it seems to be the most easily accessible medium through which Chinese intelligence services conduct their cyber-espionage attacks. Chinese intrusions happen most frequently with Microsoft products, but that is likely due to the prolific nature of Microsoft software around the world where dozens of brands use Microsoft as their software license.

Huawei hardware is very easily accessed by the Chinese intelligence services. Given the association of high-level executives with the Chinese Communist Party, and the Chinese laws that force cooperation of companies in China with all government investigations, it is difficult to believe that Huawei is remotely innocent even at the highest levels within the company. Huawei is not the only company that presents a risk.

50. Cave, "The African Union Headquarters Hack and Australia's 5G Network"; Eric Olander, "African Union Caught in Crossfire of US-China Feud over Huawei," The Africa *Report.com*, November 19, 2019, *https://www.theafricareport.com/20280/african-union-caught-in-crossfire-of-us-china-feud-over-huawei/*; Ghalia Kadiri and Joan Tilouine, "A Addis-Abeba, le siège de l'Union africaine espionné par Pékin," Le *Monde.fr*, January 26, 2018, *https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html*.

ZTE has also been documented as having very similar events occurring on their networks and any company operating out of China is not free of state influence. Chinese intelligence services need only recruit a technician or mid-level manager to carry out a majority of their attacks; Huawei, ZTE, and the others make it easily accessible by geography alone.[51]

Major Findings

This paper finds multiple major implications and makes three major conclusions resulting from significant research about the original research question: "the proliferation of technology – made by Chinese companies – in smart cities." This paper does not seek to make enemies; it exists merely to provide facts and analysis on the topic of the research question. It is the responsibility of the reader to consider the facts, sources, analysis, and conclusions presented by this paper, and then to draw their own conclusions from there. This paper largely does not contradict or part from the broader assessments made by the United States Intelligence Community (USIC) in the Worldwide Threat Assessment of the US Intelligence Community.

Chinese Owned Companies and the Risk of Cyber-Espionage to Critical Infrastructure

This paper assesses with high confidence that the use of critical network infrastructure made by Chinese owned companies presents a severe cyber-espionage threat to the U.S. and U.S. allies. The threat is somewhat mitigated by the ongoing blacklist of Chinese companies like Huawei and ZTE however, because U.S. allies such as the UK, Germany, and France use Chinese tech in their networks, U.S. sensitive information is still at risk of unauthorized disclosure.

Articles 11, 12, and 14 of the 2017 National Intelligence Law and Article 28 of the Cybersecurity Law of the PRC, as well as past instances of probable cyber-espionage conducted by, for, or with the knowledge of Chinese intelligence services, supports that conclusion. If the Chinese government was not involved in these previous instances of cyber-espionage, the fact remains that Huawei, ZTE, Lenovo, and other Chinese owned companies' equipment come equipped with serious security flaws which would nonetheless place users' sensitive information at risk.

51. Cave, "The African Union Headquarters Hack and Australia's 5G Network"; Robertson and Tarabay, "Chinese Spies Accused of Using Huawei in Secret Australian Telecom Hack - Bloomberg"; Lecher, "Is Huawei a Security Threat?"

5G and Internet-of-Things (IoT) Devices & Big Data

This paper assesses with high confidence that China has the capability to easily compromise 5G networks – including those which support the function of smart city IoT devices – and would further be willing to deny, degrade, or disrupt otherwise functioning smart city networks which contain Chinese company made hardware. This paper further assesses with high confidence that China would be willing to use this likely capability to conduct any number of espionage-related operations during a time of crisis, or when from their perspective, the potential rewards outweigh the potential cost.

This conclusion is supported by Articles 11, 12, and 14 of the 2017 National Intelligence Law and Article 28 of the Cybersecurity Law of the PRC, as well as past instances of probable cyber-espionage conducted by, for, or with the knowledge of Chinese intelligence services. If the Chinese government was not involved in these previous instances of cyber-espionage, the fact remains that Huawei, ZTE, and other Chinese owned companies' equipment come equipped with serious security flaws which would nonetheless place smart cities at risks ranging from complete denial of service, moderate to severe degradation, or partial disruption of key services. This conclusion is also supported by the fact that smart city IoT sensors will continue to operate not only wirelessly but utilizing 5G networks' low-band frequencies for the foreseeable future.

Identifying Persons of Interest

This paper assesses with very high confidence that China will utilize smart city technology to identify, track, and reconnoiter "U.S. Persons of Interest" both within their own political borders, and anywhere which they have both a high-level of influence with the host country, and a perceived threat to their interests. Surveilled individuals may include but are not limited to diplomats and embassy personnel, politicians, private business leaders and representatives, students in STEM degree fields, and anyone associated with a foreign military. It is also likely that they will utilize every resource of their intelligence collection capability including but not limited to biometrics, financial records, social media and internet search history, foreign travel history, and professional work history to develop profiles on potential sources of valuable information to the Chinese government.

As China continues to develop and implement the technology that supports its social credit score system,

the ability of their intelligence services to surveil potential targets of interest will increase significantly. The number of operational smart cities in China will also very likely increase over a short period of time and will serve to support the CCP in law enforcement and intelligence activities. Finally, as China continues to exert its influence across the globe, the risk of Chinese intelligence services utilizing smart city technology outside their borders will also increase significantly.

Additional Analysis

The single greatest detriment to this paper is the lack of a 'smoking gun.' Several documents and sources reveal that at least to some extent, there are links between the CCP and the listed companies, especially Huawei. There are connections of at least limited use of the Chinese military and intelligence services to gain advantageous information on behalf of Chinese companies. There are connections between Huawei and its use of AI and Facial Recognition Software to identify persons based on numerous different indicators within a profile; that could be detrimental to U.S. and allied intelligence operations within China and elsewhere that Chinese tech is present. Despite all these indications, the level at which and the extent to which these operations occur and are approved, is unclear. The apparent/seemingly decentralization of these operations makes broad and complete accountability for these violations of the law difficult to enforce due to the plausible deniability of the greater Chinese government and CCP writ-large, as well as that of Huawei and other Chinese companies. However, these case studies demonstrate a propensity for high-risk of compromise by carrying Chinese technology in one's telecommunications network; regardless of whether the company is cooperating. It is also worth noting, that despite the denial by the Chinese government in being complicit in, guilty of, or otherwise, of spying, that they would be stupid not to take advantage of that intelligence data goldmine.

CONCLUSION

The analysis indicates that the Chinese government could easily exploit Huawei's presences on U.S. networks by intercepting sensitive communications; conducting cyber operations; degrading, disrupting, denying, or destroying critical city services in times of national emergency; and to collect intelligence. Extensive support from the Chinese government allows Huawei to under bid their competitors and the Chinese military has been known to conduct industrial/economic espionage – Cisco, T-Mobile, and Motorola for example – on behalf of Chinese private companies. Furthermore, even if Huawei wanted to refuse cooperation in enabling the Chinese government's spying apparatus, there is little they could do to deny the CCP access due to the national security and cyber security laws signed in 2017. The laws require them to comply with any government investigation. Last, none of these allegations based on the analysis of this paper, are inconsistent with the previous espionage behavior of China; this is merely an evolution of tradecraft – a new medium – the Chinese government can to exploit.

Referring to the main research question for this analysis – the use of Chinese commercially made telecommunications equipment affects the probability of compromise by Chinese intelligence services, and whether other countries' products could be just as vulnerable – the answer is clear. The use of Chinese commercially made telecommunications equipment increases the probability of compromise by the Chinese intelligence services, even if the Chinese company is not deliberately enabling the compromisation. The ease of access Chinese intelligence has to working level technicians and middle managers – even just geographically – make clandestine cyberattacks easy to conduct with Huawei equipment. Furthermore, as Huawei – at a minimum – incentivizes or has incentivized the theft of competitor intellectual property, it is likely that Huawei is to blame for at least some espionage activity.

Regarding sub-question #1 – what telecommunications components are most likely to be compromised by Chinese intelligence services (broadly) both prior to product purchase (e.g., preloaded backdoor), and after network installation (e.g., brute force hacking, signals intelligence collection, etc.)? This analysis finds that most frequently when Chinese tech is compromised, it is not any specific component or product. More broadly, it is the software that tells the physical device how to operate. Therefore, components are likely equally vulnerable to compromise whenever a software update/patch is sent out from the managing company.

Regarding sub-question #2 – how might China use intelligence collected while transiting networks containing critical components (hardware/software) designed and manufactured in China? This analysis finds that most frequently, the intelligence targeted is the intellectual property of other foreign compa-

nies with the goal of enhancing Chinese companies' advantage in global markets and in international business deals. Other intelligence of value to the Chinese government gathered through the exploitation of Chinese technology could include but is not limited to suppression of minority groups and political opposition; enhancing Chinese influence abroad by accessing critical information to aide in business and security deals; targeting foreign surveillance teams/individuals as a function of their counterintelligence operations; harming the national security of U.S. allies by being able to disrupt, degrade, or deny access to critical telecommunications networks during a time of crisis or to force ransom and other capitulations (especially in the 5G networks that enable Smart City infrastructure)

FUTURE RESEARCH

This topic is huge and cannot be adequately addressed with nuanced and actionable recommendations in one master's research paper. Instead, this research should be considered a starting point from which to expand. One route, should be to focus on this topic specifically from a counterintelligence perspective, giving information to the correct personnel within the USIC so that tradecraft may be developed as a reasonable countermeasure to the multifaceted threats presented by Huawei and Chinese technical surveillance means through smart city technology: especially regarding FRS and other technical person-identifying technology. The other route is to provide an economic assessment and full-scope analysis of smart cities, predictions for the future of the technology, and information that would be best served to the policy maker in directing the future of American smart cities.

Bibliography and Glossary available online at *https://tinyurl.com/ftmaavsa*.

AUTHOR NOTES: This article is based on work conducted as a candidate for a Master of Professional Studies (MPS), in the Applied Intelligence Capstone Course, at Georgetown University School of Continuing Studies.

The author wishes to thank his Review Committee, Department Chair & Director of MPAI Program Professor Frederic Lemieux PhD; Capstone Paper Advisor: Adrianne Romero; and External Reviewer & Second Reader: Katrina Lewis.

1LT Jason Harriman is currently an Officer in the U.S. Army's 4th Infantry "Ivy" Division. He joined the U.S. Army in 2014 as a Signals Intelligence Collector and supported Special Operations Forces and maneuver units in Northern Iraq from 2016-2017. Jason graduated from Embry-Riddle Prescott, AZ campus in 2020 with a BS in Security & Intelligence and an Active Duty commission into the U.S. Army. In 2022, he graduated from Georgetown University in Washington D.C. with his Master's in Applied Intelligence. Jason has also served in DIA's Office of Counterintelligence.