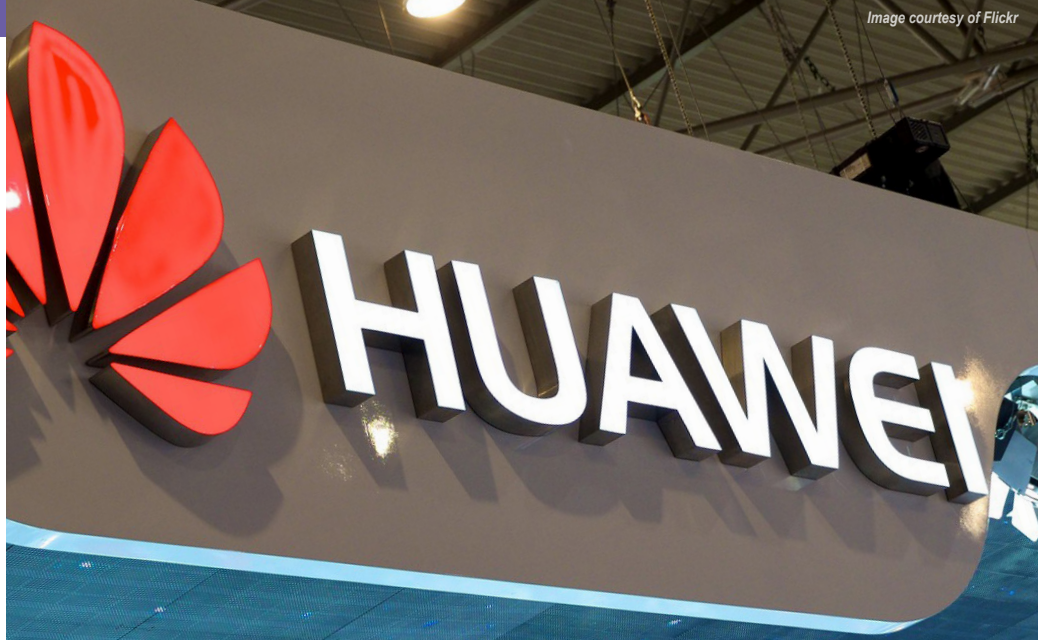


# HUAWEI: EXPANDING CHINA'S TECHNOLOGY WEB

by Chief Warrant Officer 4 Charles Davis



## Introduction

In 2019, the *Journal of Political Risk* asserted Huawei was the most valuable telecommunications company worldwide. The company's net worth was estimated at US\$38 billion, controlling 10 percent of the global smartphone market with a compound annual revenue growth of 26 percent.<sup>1</sup> Huawei's 2021 annual report indicated that it provided telecommunications connectivity to more than 70 countries and regions.<sup>2</sup> Additionally, the company reported significant gains in artificial intelligence development and integration, boasting a top 30 listing as a Super Artificial Intelligence Leader.<sup>3</sup>

In September 2021, both Huawei's high-resolution millimeter wave radar and its artificial intelligence algorithm-based cloud warning technology won the Global New Energy Vehicle Cutting-edge and Innovative Technologies Award from the World New Energy Vehicle Congress.<sup>4</sup> Soon, Huawei expects to achieve automation, self-healing, self-optimization, and autonomy for its Autonomous Driving Networks. These milestones will incorporate four features: advanced intelligent sensing, digital mapping, self-learning, and adaptive decision making.<sup>5</sup> Given such significant global success, why would the United States be concerned with Huawei leading the development of 5<sup>th</sup> generation mobile network (5G) capabilities in America? The answer is clear: Global industries and government infrastructure are increasingly relying on mobile networks. 5G network integration could pose significant domestic, strategic, and national security risks. Which means the United States needs a clear understanding of the relationships between nation states and corporations that develop those technologies.

## Private Company or Arm of the State?

Huawei was founded in Shenzhen, Guangdong, China, in 1987 by Ren Zhengfei, a former People's Liberation Army officer. The company is officially owned by 80,000 of its 180,000 employees. However, Zhengfei maintains veto power over the majority in all organizational decisions. Uncertainty over Zhengfei's relationship with the Chinese government and lack

of corporate transparency has resulted in the United States banning Huawei from bidding on United States government contracts. The ban also imposes severe restrictions on federal employees' use of Huawei's products.

The Chinese government may feel motivated to guide and support Huawei's business dealings and contracts because of traditional Chinese Communist Party (CCP) behavior. The People's Republic of China would leverage the Belt and Road Initiative to integrate and strengthen its relationship with Huawei. In his 2019 remarks on National Security and Foreign Policy Implications, Dr. Christopher Ford, then Assistant Secretary of State for International Security and Non-proliferation, stated:

*Though they may have formally private ownership and operate in the national and in the international marketplace, global Chinese firms—including Huawei—are in key ways not genuinely private companies and do not make decisions entirely for economic and commercial reasons. Whether de facto or de jure, such giants can in some important respects or for some purposes act as arms of the state—or, more precisely, the Chinese Communist Party, to which the Chinese state apparatus is itself subordinate.<sup>6</sup>*

Members of Congress and several key partners from intelligence organizations echoed Dr. Ford's observations and concerns.

## U.S. Congress Investigates Huawei

Huawei's first red flag appeared in 2007. The Congressional Research Service report, *Huawei and U.S. Law*, indicated Huawei partnered with American private investment firm Bain Capital LP to acquire an ownership interest in 3Com Corporation, an American digital electronics firm. The deal raised national security concerns because 3Com provided cybersecurity systems to the U.S. military.<sup>7</sup> By 2008, Bain Capital decided the partnership was too risky and dropped its bid for 3Com. After failed partnering attempts with Sprint

Corporation in 2010 and 3Leaf Systems in 2011, Ken (Houkun) Hu, the technologies chairman for Huawei USA, wrote an open letter to the U.S. Government.<sup>8</sup> In an effort to find some way to compete in the U.S. market, Hu denied security concerns and offered a formal investigation to alleviate any reservations.

The U.S. Congress established a committee and ordered a review to determine the relevancy and degree of threat associated with allowing Huawei to participate in government contracts. The committee documented numerous concerns with Huawei's level of cooperation and veracity during the investigation. Additionally, former Huawei employees provided internal documents asserting Huawei provides special network services to an elite cyber-warfare unit within the People's Liberation Army and still others provided information on continued incidents of alleged visa violations.<sup>9</sup> Interviews further suggested that the alleged visa violations primarily involved employees brought to the United States as engineers, who were not serving in that capacity.

The Congressional report further states that "throughout the investigation, Huawei consistently denied having any links to the Chinese government and maintains that it is a private, employee-owned company."<sup>10</sup> However, current and former employees of Huawei USA confirm it is "managed almost completely by the Huawei parent company in China,"<sup>11</sup> which is counter to Huawei's claim that its United States operations are largely independent of the parent company. However, Huawei's leadership did concede the CCP maintains a party committee within the company but did not provide an explanation of the functions those representatives perform.

Ultimately, the congressional committee determined:

*Huawei operates in what Beijing explicitly refers to as one of seven 'strategic sectors.' Strategic sectors are those considered as core to the national and security interests of the state. In these sectors, the CCP (Chinese Communist Party) ensures that 'national champions' dominate through a combination of market protectionism, cheap loans, tax and subsidy programs, and diplomatic support in the case of offshore markets. Indeed, it is not possible to thrive in one of China's strategic sectors without regime largesse and approval.*<sup>12</sup>

The committee submitted its report in 2012.

## **Australia's Concerns About Huawei**

Earlier in 2012, elements of the Australian Signals Directorate contacted United States partners indicating they had detected a sophisticated intrusion within Australia's telecommunications systems. The Australian Signals Directorate was confident the incident was initiated during a software update from Huawei, which included malicious code. Numerous former national security officials confirmed receiving briefings about the breach from Australian and United States agencies from 2012 to 2019.<sup>13</sup> "Digital forensics on those systems revealed

only fragments of the malicious code's existence, and investigators reconstructed the attack using a variety of sensitive sources, including human informants and secretly intercepted conversations, the former officials said."<sup>14</sup>

Details about the breach of Australia's telecommunications system suggest the malicious code worked much like a traditional wiretap. The code reprogrammed infected equipment to record all communications and route those recordings back to China. A self-erasing program activated after several days of data capture, resulting in much of the code being deleted.<sup>15</sup> Coincidentally, the Australian Signals Directorate's investigation determined involvement by Huawei's system maintenance engineers in espionage.<sup>16</sup> This information seems to support the visa violation allegations presented in the U.S. Congressional investigation.

By 2017 Australia's then Prime Minister, Malcolm Turnbull, was faced with tough decisions about 5G integration across the Australian continent. Given the events of 2012 he directed the Australian Signals Directorate to "red team" courses of action should China leverage its relationship with Huawei. The team determined, "if that government has sway over a 5G vendor in the country it wants to strike... 'you can get there quicker from flash to bang with zero cost of entry.' It could be done with a simple instruction to the company operating in the target nation's 5G system."<sup>17</sup> The consequences of a hypothetical, yet foreseeable, attack of this sort would not just be about intercepting information. An attack could disrupt sewage pump stations, clean water supply systems, public transportation dispatching, electric vehicle operation, and interfere with networks supporting critical economic functions. Ultimately, the red team identified more than 300 risks and had significant difficulty in trying to reverse engineer the company's design to identify potentially malign code.

The United States and Australia are not alone in their concerns over the risks associated with reliance on Huawei's 5G infrastructure. In Jan-Peter Kleinhans's policy recommendations for Europe's 5G development, he stated that "the IT security of mobile networks must be addressed on four different levels—standards, implementation, configuration, operations."<sup>18</sup> Kleinhans also described these networks as "highly modular and complex networks that blur the line between vendor and operator,"<sup>19</sup> expressing the difficulties in defining and clarifying the lines of responsibility. RAND analyst Timothy Heath assessed that "as an equipment vendor, it is technically possible for Huawei to conduct espionage through the network, or even for it to disrupt communications with disastrous consequences. As more devices are connected to the internet, including autonomous vehicles and electrical grids, this threat becomes all the more real."<sup>20</sup> This gray zone provides China significant operating space and plausible deniability for companies like Huawei.



Industry leading security experts also took a hard look at Huawei's potential vulnerabilities. Finite State and ReFirm Labs, acquired by Microsoft in 2021, did their own analysis using new automated searches of firmware files. Terry Dunlap, Refirm Labs' co-founder, indicated that in about 30 minutes his program could obtain a "complete profile on passwords that may have been accidentally left in, cryptographic keys that may or may not be warranted [and], ... insecure coding practices that could be exploited."<sup>21</sup> In less than 2 days' time, Finite State was able to review more than 500 Huawei enterprise networking products from business systems. On average each device had 102 vulnerabilities, at least a quarter of them severe enough to let a hacker easily gain full access.<sup>22</sup>

### Not Everyone Wants to Limit Huawei's Access

Not everyone is on board with restricting Huawei's access and limiting the company from competing and providing their advanced solutions. The Swedish Institute of International Affairs is not convinced a ban of Huawei will reduce any threats of espionage from China. "We do not follow the mainstream argument put forward by critics of a ban that the use of Huawei technology is essential to avoid losing ground in the development and roll-out of 5G."<sup>23</sup> The Swedish Institute of International Affairs is especially concerned over the potential political repercussions associated with negative action against the company. This is not surprising because President Xi Jinping is wholly invested in Huawei securing its place as the leader in the global internet, going so far as to suggest to former President Trump that a ban would be harmful to bilateral relations.<sup>24</sup> Implications for the European Union are precarious at best. Poland and the Czech Republic are firmly in line with the United Kingdom, Australia, and the United States in what has become a 60 State coalition, while Germany, France, Italy, and Portugal are leaning toward some degree of inclusion for Huawei.

For its own part, Huawei continues to counter any negative image presented by the United States and its partners. In 2019, Huawei commissioned Oxford Economics to conduct a study of the implications and impacts of preventing a key 5G supplier from building infrastructure. The study, released in December 2019 finds, "restricting a key supplier of 5G infrastructure from helping to build a country's network would increase that country's 5G investment costs by between 8% to 29% over the next decade."<sup>25</sup> It further asserts that restricting competition and participation would delay 5G access to millions and would slow technological innovation and growth. It is not surprising the study favors allowing all competitors equal access to countries developing 5G capabilities and is in line with information management and narrative framing common to the CCP. The U.S. Government does not share this assessment.

## U.S Restrictions Through the National Defense Authorization Act

It is doubtful these findings will sway any of the 60 countries already committed to protecting their domestic infrastructure from China's threat. Over the past 4 years the United States has continuously elevated restrictions through the National Defense Authorization Act (NDAA). The 2018 NDAA prohibits the Department of Defense (DoD) from procuring certain telecommunications equipment or services from Huawei and others as part of DoD's missions related to nuclear deterrence and homeland defense.

The 2019 NDAA included a more comprehensive set of restrictions for Huawei, which encompassed the Executive Branch. Executive agencies are no longer allowed to procure systems that contain Huawei's equipment or services, nor are they allowed to contract with companies using Huawei equipment or services.<sup>26</sup>

The 2020 NDAA restricts the Secretary of Commerce's ability to remove Huawei from the Entities List, requiring four conditions to change its status:

- ◆ Resolution by Huawei of the charges that were the basis for its addition to the Entity List.
- ◆ Resolution by Huawei of any other charges that it violated U.S. sanctions.
- ◆ Implementation of regulations that sufficiently restrict exporting to, and importing from, the United States items that would pose a national security threat to U.S. telecommunications systems.
- ◆ Mitigation by Commerce, to the maximum extent possible, of other threats to U.S. national security posed by Huawei.<sup>27</sup>

### U.S. Department of Commerce Entities List

The Entity List is a tool utilized by the Department of Commerce's Bureau of Industry and Security to restrict the export, re-export, and transfer (in-country) of items subject to the Export Administration Regulations to persons (individuals, organizations, or companies) reasonably believed to be involved, or to pose a significant risk of becoming involved, in activities contrary to the national security or foreign policy interests of the United States. Additional license requirements apply to exports, re-exports, and transfers (in-country) of items subject to the Export Administration Regulations to listed entities, and the availability of most license exceptions is limited.<sup>28</sup>

The U.S. Senate is proposing cooperative agreements with partner nations and reporting requirements to monitor Huawei's capabilities and intentions in Senate bill S.1260, *United States Innovation and Competition Act of 2021*.<sup>29</sup> Additionally, Executive Order 14032, *Addressing the Threat From Securities Investments That Finance Certain Companies of the People's Republic of China*, prohibits U.S. investments in Chinese companies that undermine the security or democratic values of the United States and its allies, effective June 3, 2021.<sup>30</sup>

## Huawei's Technology in the United States

Despite recent prohibitions, Huawei technology remains in the U.S. infrastructure. Many rural wireless carriers use the technology in their networks, predominantly because of the low price afforded to these groups. Restricted budgets continue to create opportunities for exploitation. In 2018, 25 percent of the Rural Wireless Association members reported current deployment of equipment from Huawei, or its sister company ZTE, in their networks.<sup>31</sup> Huawei equipment in these rural areas posed a potential threat to several military installations, as Bloomberg Law noted in November 2019.<sup>32</sup>

Federal Communications Commission and Congressional concerns regarding the Huawei presence in rural carriers resurfaced upon the release of a Cable News Network (CNN) special report in July 2022. The CNN investigative piece asserts that the Federal Bureau of Investigations identified, "Chinese-made Huawei equipment atop cell towers near military bases in the rural Midwest."<sup>33</sup> The investigation determined the components could capture or disrupt restricted DoD communications. Of particular concern is U.S. Strategic Command, which oversees the country's nuclear weapons and could potentially be affected by the technology's vulnerabilities.<sup>34</sup> Additionally, the CNN report stated that "around 2014, Viaero [the largest regional provider in the area] started mounting high-definition surveillance cameras on its towers to live-stream weather and traffic, a public service it shared with local news organizations. ... But they were also inadvertently capturing the movements of US military equipment and personnel, giving Beijing—or anyone for that matter—the ability to track the pattern of activity between a series of closely guarded military facilities."<sup>35</sup>

## Options to a Persistent Threat

The United States counterintelligence community identifies China as the world's most active and persistent perpetrators of economic espionage.<sup>36</sup> Former National Counterintelligence Executive, Mr. Robert Bryan, testified, Chinese intelligence services, as well as private companies and other entities, often recruit those with direct access to corporate networks to steal trade secrets and other sensitive proprietary data. China prizes comprehensive and effective cyberspace and human-related espionage; incorporated with sophisticated technology, it retains the capability to introduce malicious hardware into both Chinese manufactured components and vendor serviced systems. These results can be catastrophic to private industry and state government, leaving both inoperable, ineffective, and unaware of the threat until it is too late.

To provide a secure and competitive option to Huawei, DoD is continuing industry partnerships. In October 2020, US\$600 million dollars in research funding was earmarked for 5G experimentation. This development represents the largest full scale 5G dual use testing in the world. "Projects

will include piloting 5G-enabled augmented/virtual reality for mission planning and training, testing 5G-enabled Smart Warehouses, and evaluating 5G technologies to enhance distributed command and control".<sup>37</sup> Test sites span across all Service components including Naval Base San Diego, California; Marine Corps Logistics Base Albany, Georgia; Nellis Air Force Base, Nevada; Hill Air Force Base, Utah; and Joint Base Lewis-McChord, Washington.

Most recently, an August 2, 2022, press release indicates DoD is directing innovative efforts toward Open6G with open radio access networks (Open RAN).<sup>38</sup> Northeastern University's Kostas Research Institute will manage the project. Initiatives such as these ensure the United States is matching strides with pacing threats while protecting American infrastructure, financial institutions, and technology. 🌟

## Endnotes

1. Douglas Black, "Huawei and China: Not Just Business as Usual," *Journal of Political Risk* 8, no. 1 (January 2019), <https://www.jpolrisk.com/category/diplomacy/page/8/>.
2. Huawei Investment & Holding Co, Ltd., *2021 Annual Report*, 7, <https://www.huawei.com/en/annual-report/2021>.
3. Ibid., 68.
4. Ibid., 68.
5. Ibid., 70.
6. Dr. Christopher Ashley Ford, "Huawei and Its Siblings, the Chinese Tech Giants: National Security and Foreign Policy Implications," (remarks, Multilateral Action On Sensitive Technologies [MAST] Conference, Loy Henderson Auditorium, Department of State, Washington DC, September 11, 2019), <https://2017-2021.state.gov/huawei-and-its-siblings-the-chinese-tech-giants-national-security-and-foreign-policy-implications/index.html>.
7. Library of Congress, Congressional Research Service, *Huawei and U.S. Law*, Stephen P. Mulligan and Chris D. Linebaugh, CRS Report R46693 (Washington, DC: Office of Congressional Information and Publishing, February 23, 2021), <https://crsreports.congress.gov/product/pdf/R/R46693>.
8. Ken Hu, "Huawei Open Letter," <https://www.wsj.com/public/resources/documents/Huawei20110205.pdf>.
9. Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, 112<sup>th</sup> Cong., 2<sup>nd</sup> sess., October 8, 2012, 25, 35, [https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20\(final\).pdf](https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf).
10. Ken Hu, "Huawei Open Letter."
11. Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues*, 13.
12. John Lee, "The Other Side of Huawei," *Business Spectator*, March 30, 2012.
13. Jordan Robertson and Jamie Tarabay, "Chinese Spies Accused of Using Huawei in Secret Australia Telecom Hack," *Bloomberg*, December 16, 2021, <https://www.bloomberg.com/news/articles/2021-12-16/chinese-spies-accused-of-using-huawei-in-secret-australian-telecom-hack>.
14. Ibid.
15. Ibid.



16. Anees, "Huawei products-Australia and the United States grasped from 2012," Quepan, n.d., <https://quepan.net/post/huawei-products-australia-and-the-united-states-grasped-from-2012>.

17. Peter Hartcher, "Huawei? No way! Why Australia banned the world's biggest telecoms firm," *The Sydney Morning Herald*, May 21, 2021, <https://www.smh.com.au/national/huawei-no-way-why-australia-banned-the-world-s-biggest-telecoms-firm-20210503-p57oc9.html>.

18. Jan-Peter Keinans, *Whom to trust in a 5G world? Policy recommendations for Europe's 5G challenge* (Berlin, Germany: Stiftung Neue Verantwortung, 2019), <https://www.stiftung-nv.de/de/publikation/whom-trust-5g-world-policy-recommendations-europes-5g-challenge>.

19. Ibid.

20. Kate O'Flaherty, "Huawei Security Scandal: Everything You Need to Know," *Forbes*, February 26, 2019, <https://www.forbes.com/sites/kateoflahertyuk/2019/02/26/huawei-security-scandal-everything-you-need-to-know/?sh=7d3239d773a5>.

21. Sydney J. Freedberg Jr., "Hacker Heaven: Huawei's Hidden Back Doors Found," *Breaking Defense*, July 5, 2019, <https://breakingdefense.com/2019/07/hunting-huaweis-hidden-back-doors/>.

22. Ibid.

23. Tim Rühlig and Maja Björk, *What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe* (Stockholm, Sweden: The Swedish Institute of International Affairs, 2020), <https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/2020/ui-paper-no.-1-2020.pdf>.

24. Peter Hartcher, "Huawei? No way!"

25. Oxford Economics, *The Economic Impact of Restricting Competition in 5G Network Equipment: An Economic Impact Study*, December 2019, <https://www.oxfordeconomics.com/resource/economic-impact-of-restricting-competition-in-5g-network-equipment/>.

26. Library of Congress, Congressional Research Service, *Huawei and U.S. Law*.

27. *National Defense Authorization Act for Fiscal Year 2020*, Public Law 116-92, Sec. 12601 (a) (1), (2), (3), (4), <https://www.govinfo.gov/content/pkg/PLAW-116publ92/html/PLAW-116publ92.html>.

28. Department of Commerce, "Commerce Department Adds 34 Entities to the Entity List to Target Enablers of China's Human Rights Abuses and Military Modernization, and Unauthorized Iranian and Russian Procurement," *Office of Public Affairs*, July 9, 2021, <https://www.commerce.gov/news/press-releases/2021/07/commerce-department-adds-34-entities-entity-list-target-enablers-chinas>.

29. Senate, *United States Innovation and Competition Act of 2021*, S 1260, 117<sup>th</sup> Cong., 1st sess., introduced in Senate on April 20, 2021, <https://www.congress.gov/bill/117th-congress/senate-bill/1260/text>.

30. "Executive Order 14032 of June 3, 2021, Addressing the Threat From Securities Investments That Finance Certain Companies of the People's Republic of China," *Code of Federal Regulations*, title 3 (2021): 30145-30149, <https://www.federalregister.gov/documents/2021/06/07/2021-12019/addressing-the-threat-from-securities-investments-that-finance-certain-companies-of-the-peoples>.

31. Mike Dano, "Huawei equipment currently deployed by 25% of U.S. rural wireless carriers, RWA Says," *Fierce Wireless*, December 11, 2018, <https://www.fiercewireless.com/wireless/huawei-equipment-currently-deployed-by-25-u-s-rural-wireless-carriers-rwa-says>.

32. *Bloomberg Law*, "FCC Wants to Know if Huawei Gear Is near U.S. military Bases," November 5, 2019, <https://news.bloomberglaw.com/tech-and-telecom-law/fcc-wants-to-know-if-huawei-gear-is-near-u-s-military-bases>.

33. Kate Bo Lillis, "CNN Exclusive: FBI investigation determined Chinese-made Huawei equipment could disrupt US nuclear arsenal communications," *CNN*, Politics, July 25, 2022, <https://www.cnn.com/2022/07/23/politics/fbi-investigation-huawei-china-defense-department-communications-nuclear/index.html>.


34. Ibid.

35. Ibid.

36. Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011* (Washington, DC, October 2011), [https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103\\_report\\_fecie.pdf](https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf).

37. Department of Defense, "DOD Announces \$600 Million for 5G Experimentation and Testing at Five Installations," October 8, 2020, <https://www.defense.gov/News/Releases/Release/Article/2376743/dod-announces-600-million-for-5g-experimentation-and-testing-at-five-installati/>.

38. Department of Defense, "Three New Projects for DOD's Innovate Beyond 5g Program," August 2, 2022, <https://www.defense.gov/News/Releases/Release/Article/3114220/three-new-projects-for-dods-innovate-beyond-5g-program/>.



CW4 Charles Davis serves on the faculty of the Warrant Officer Career College. He currently instructs International Strategic Studies at all levels of Warrant Officer Education. CW4 Davis is a graduate of the U.S. Army War College Strategic Broadening Program and holds a master's degree with honors in intelligence studies from American Military University. CW4 Davis is also a recipient of the Military Intelligence Corps Knowlton Award.