TRILATERAL CYBER SECURITY COMMISSION

NATIONAL SECURITY STRATEGY FOR 5G

FINDINGS & RECOMMENDATIONS ON MEETING THE 5G CHALLENGE

DECEMBER 2019

TRILATERAL CYBER SECURITY COMMISSION

The Trilateral Cyber Security Commission was convened and is supported by the Sasakawa Peace Foundation USA. Sasakawa USA is dedicated to strengthening U.S.-Japan relations through education, programs and research. Improved cyber security is an imperative for both countries, as well as for their partners in Europe. The Commission has brought together prominent officials and leaders from government, business and universities to make recommendations for coordinated policies and actions that will benefit the United States, Japan and like-minded European countries.

COMMISSIONERS

- Admiral Dennis Blair (Ret.), Distinguished Senior Fellow (Non-Resident), Sasakawa Peace Foundation USA
- The Hon. Michael Chertoff, Executive Chairman, Chertoff Group
- Arthur Coviello, Jr., Venture Partner, Rally Ventures
- Hiroshi Ito, CTO, FireEye Japan
- Dr. Jamie Saunders, Visiting Professor, University College London
- Dr. Satoru Tezuka, Professor, Keio University

DIRECTORS

- Executive Director – William Roth, Non-Resident Fellow for Cybersecurity, Sasakawa Peace Foundation USA
- Director for Japan – Kazuo Noguchi, Senior Researcher, Keio University

TECHNICAL ADVISORS

- Duncan Sparrell, former Distinguished Senior Network Engineer, AT&T
- Dr. Linton Wells, Executive Advisor, George Mason University C4I & Cyber Center

CONTENTS

EXECUTIVE SUMMARY

The Trilateral Cyber Security Commission was formed to make recommendations to the governments of the United States, Japan, and like-minded European countries individually and collectively to improve the security of their information networks. Some of the most critical challenges to all these countries are the economic and security risks of future 5G networks. These rapidly developing networks will become a new and dominant form of critical infrastructure. Unless the free market democratic countries can develop polices and take actions in the near term, China is poised to dominate this emerging market and could use its position to undermine the national security of its adversaries.

To develop effective policies for the long term, it is necessary to differentiate between the systemic information security threat of integrating foreign-made gear into 5G networks, on the one hand, and the economic dangers of China's government-orchestrated unfair trade practices and intellectual property theft, on the other. In the midst of a trade dispute driven by China's massive trade imbalance with the West, there is an understandable temptation to handle all three related challenges—information security, mercantilism and trade deficits—with a single approach. However, a sustained successful response requires that they be treated separately. The following observations summarize the major points supporting this conclusion and ultimately, drive the Commission's recommendations on 5G:

- 5G networks will be a critical part of the world's cellular and digital infrastructure in the near future, hosting new forms of automated and device communications and creating a new USD $250 billion market.

- Like current cellular networks, 5G networks are at risk if they are built with hardware and software from foreign companies subject to unfriendly government pressure or that are not engineered to high security standards.

- China is engaged in an orchestrated effort to use both legal and illicit means to dominate the world's 5G markets using control of its domestic market, subsidies to IT national champions such as Huawei and ZTE, and acquisition of Western technology through coercion and espionage. Without concerted counters by the free market democratic countries, China may well achieve its ambitious goal.

- Beyond the economic consequences, Chinese domination of the international 5G market poses national security risks. Huawei and ZTE have a track record of supporting Beijing's foreign policy goals by engaging in activities such as evasion of international sanctions. There is every reason to believe they would support Chinese government requests for network access.

- Economic and national security risks are related, but some risk factors reflect China's state-sponsored economic strategy and others reflect systemic risks inherent in 5G evolving into a critical infrastructure.

- The United States and most of its allies lag behind in developing complete 5G systems that can be sold at scale in their own countries and compete in international markets.

- Private companies in free-market democracies cannot defend themselves alone against the coordinated threat of Chinese national champions and the Chinese government working together.

- The policies and actions of the United States, Japan, and like-minded European countries have enjoyed some success in countering China's mercantilist policies in the 5G industry but must be improved to pace this threat.

Informed by these insights, the Commission recommends the United States, Japan, and like-minded governments in Europe and elsewhere take a series of domestic and coordinated multilateral actions. The objectives are not only to protect their 5G networks, but also to support Western firms in competing fairly to deliver 5G solutions around the world.

OUR RECOMMENDATIONS:

1. Establish a two-prong domestic review mechanism to review 5G network procurement from foreign suppliers to ensure that telecom carriers purchase equipment (1) not at high risk of compromise through pressure on the supplier by an unfriendly government and (2) built with sufficient security features to minimize the risk for opportunistic hackers to compromise the gear.

2. Strengthen domestic policies and actions to penalize foreign firms supplying 5G equipment that benefit from illegal subsidies from their home governments or that conduct illegal activities such as IP theft.

   A. Establish a process for rapid government decisions and imposition of penalties by experienced officials, shifting the burden of proof from the domestic victim to the foreign supplier.

   B. Tailor penalties for specific companies to the scale of economic damage.

3. Promote the development of a robust, open domestic 5G sector in the free market democracies capable of building alternative 5G solutions.

   A. Support open protocols to enable 5G gear to intercommunicate with 3G and 4G networks in order to reduce "vendor lock-in" and the resulting the barrier to entry for new 5G firms.

B. Support an open and modular architecture for 5G networks that permits carriers to integrate equipment from various sources without significant integration costs

C. Create investment incentives designed to encourage domestic companies and overseas firms from trusted nations to invest in 5G technologies and networks

D. Encourage industry cooperation in forming 5G system suppliers by the selective use of waivers to federal and state antitrust law as was done in the US with the Cybersecurity Information Sharing Act of 2016

E. Incentivize participation in domestic 5G system ventures to qualified foreign firms from trusted allies.

4. Fund basic research in critical 5G technology not taking place in the private sector such as:

   A. Improved technology for spectrum sharing in the prime 5G frequency bands.

   B. Secure communications over untrusted networks.

   C. Identification and segregation of "high risk" components in 5G networks for which foreign components carrying high political risk should never be used, and "lower risk" components subject to lower security requirements.

5. Establish a "5G International Security Council (5G ISC)" as the primary mechanism for international coordination of 5G security and trade policies of the member states. The council would include government officials with national security, economic, and digital infrastructure regulation responsibilities, as well as representatives from major 5G providers and vendors. The 5G ISC would have the following responsibilities:

   A. Coordination of the criteria to be used for each member country's review of the political risk of foreign 5G equipment suppliers, along with comparison and potential coordination of specific results of reviews.

   B. Coordination of technical standards used to assess the security risk of 5G vendor hardware and software, along with comparison and potential coordination of specific results of reviews.

   C. Continuous sharing of threat and risk assessments among the council members.

   D. Coordination on spectrum allocation issues.

   E. Developing and coordinating opportunities for partnerships among member nation's companies to facilitate development of robust, price-competitive alternatives to Huawei and ZTE while ensuring any antitrust or trade treaty concerns are preemptively addressed.

F. Coordination of research into new technologies for spectrum sharing, open protocols, and secure end-to-end communications over future 5G networks for specific organizations.

G. Comparison of technical reviews and agreement on "high" vs. "low" risk components of 5G networks.

5G NETWORKS AND CHALLENGES

THE WORLD'S NEXT BIG OPPORTUNITY

Fifth generation wireless networks, or "5G," is the next big event in the growth of digital networking. 5G networks can transmit data at up to 10 times the speed (bandwidth) of 4G and respond in a tenth the time (latency). High speed, low latency 5G networks are expected to drive a new wave of technological innovation in areas such as highly automated industrial facilities, autonomous vehicles, and internet of thing (IOT) devices. Ericsson predicts that by 2023, there will be over a billion 5G users with 20% of cellular traffic carried on 5G networks.[1] This new cellular technology will not only replace existing cellular networks, but replace substantial segments of current WIFI, WIMAX, and even wired networks. Research and Markets estimates 5G's compounded annual growth rate at 97% by 2025, bringing this currently non-existent market to USD $251 billion in value.[2] MarketWatch estimates the 5G chip market alone will grow at a rate of 49% or more, reaching USD $14.5 billion by 2025.[3] All this means that the 5G rollout is the world's next gold rush.

With such a huge new market beckoning, countries have strong incentives to win market share. Many are surprised to find China poised to lead 5G development around the world. For a variety of reasons, the United States, Japan, and many European companies with strong technology sectors have failed to invest heavily in end-to-end 5G research and development. Domestic firms in these countries are prepared to build and manufacture some, but not all the

1. Ericsson, "Mobility Report," June 2018, available at: https://www.ericsson.com/assets/local/mobility-report/documents/2018/ericsson-mobility-report-june-2018.pdf

2. Research and Markets, Homepage, as of December 20, 2018, available at: https://www.researchandmarkets.com/research/k87c8n/global_data_sheet?w=4

3. Press Release, "Global 5G chipset Market to reach USD 14.5 billion by 2025," MarketWatch, June 14, 2018, 6:14 a.m. ET, available at: https://www.marketwatch.com/press-release/global-5g-chipset-market-to-reach-usd-145-billion-by-2025 2018-06-14

components of a 5G network. Meanwhile, these governments' primary role has been to auction radio-frequency spectrum for use by telecoms building 5G networks, assuming that the private sector will take the lead on all other aspects of fielding the systems. This is in stark contrast to China, where the government identified 5G technology as one of the global high-tech markets for Chinese firms to dominate. Western firms are poorly positioned to take on a China's government-funded 5G champions and need support to develop effective 5G alternatives. This reality must influence policymakers' attempts to deal with the threat from China.

Benefits of Being First to Market

5G plans for both governments and companies are heavily influenced by the experiences of earlier cellular technologies. U.S.-developed 4G technologies became dominant around the world (including many components sold or licensed to competitors in China) because the United States was quick to integrate 4G services into existing cellular networks, giving its carriers the revenue to drive new product development and develop working implementations of 4G standards. The story was very different for 3G. U.S.-designed proprietary protocols such as CDMA, although arguably superior technologically, were expensive and unable to compete with the economies of scale that GSM created as an open standard for participating vendors.[4] Ultimately, by the time 3G transitioned to 4G, few carriers still used CDMA and those that did dropped it in favor of next-generation GSM.

The lessons of 4G and 3G seem to be that the 5G market will be dominated by the companies that can establish themselves quickly in an initial market with reasonably well performing, competitively priced equipment and then rapidly expand from that base into other international markets. As noted by the U.S. Department of Defense's Defense Innovation Board, these market leaders will be uniquely positioned to win market share by providing proven systems based on their proprietary standards to international 5G markets.[5]

Telecom carriers are rushing to introduce prototype 5G services, testing this revolutionary technology across the world. China currently has deployed by far the greatest number of systems component and equipment makers. They are building relationships with these carriers, seeing the potential for huge revenues designing and building equipment for 5G network operators and smart device and 5G IoT device manufacturers seeking to connect to them. Many telecom manufacturers and providers, including Verizon, Intel, Qualcomm, AT&T, Nokia, Samsung, Ericsson, NEC, Cisco, Deutsche Telekom, Broadcom, NTT DoCoMo, Telefonica, Alcatel-

4. It is worth noting that Europe mandated that 3G be an open specification. Sascha Segan, "CDMA vs. GSM: What's the Difference," *PC Magazine*, May 24, 2019, available at: https://www.pcmag.com/news/300986/cdma-vs-gsm-whats-the-difference

5. Defense Innovation Board, "The 5G Ecosystem: Risks & Opportunities for DoD," April 2019, p.4, available at: https://media.defense.gov/2019/Apr/04/2002109654/-1/-1/0/DIB_5G_STUDY_04.04.19.PDF

Lucent, Huawei, and ZTE, are developing 5G chips and components to meet the expected demand for 5G.[6]

The current assessment of most experts is that only a few companies—Huawei, ZTE, Samsung, Nokia, and Ericsson—have the full set of hardware and software products, along with the expertise in system installation and operation, to be major suppliers of 5G in the short term.[7] Although the United States was a 4G leader, the companies behind the U.S. success in 4G were acquired or turned to a licensing model that delegated production to overseas partners.[8] Meanwhile, U.S. carriers, who helped drive the U.S. lead in 4G by adopting the standard early, have embarked on 5G pilots, but are not yet committed to a single model for 5G in a way that will drive early innovation by their suppliers. [9] They are attempting to understand the applications that will run on 5G networks before they make the enormous investments in 5G infrastructure. In contrast, Huawei, ZTE, and Samsung are aggressively winning market share in a wide variety of overseas 4G markets at the expense of their competitors, giving them a marketing and revenue advantage for the push into 5G.[10] A large presence in existing 3G and 4G infrastructure gives firms a big technical advantage as well. Because there is no established communications API to allow 3G and 4G networks to integrate with 5G, established vendors are free to design proprietary solutions that allow their 5G equipment to easily "talk" to their 3G and 4G gear. This lowers the cost of acquisition for telecom carriers that stick with existing vendors, creating a vendor "lock-in" incentive that is an impediment to new 5G firms.

---

6. Staff, "Global 5G Infrastructure Market and 5G Servies Market 2019 Business Opportunities, Current Trends, Industry-Revenue [sic], Services, Growth-Factors [sic] and Innovative Technology by 2025," Reuters, March 26, 2019, available at: https://www.reuters.com/brandfeatures/venture-capital/article?id=93493

7. It must be noted that QualComm's chip technology is a critical component, but QualComm's business model involves a lot of licensing to manufacturing. Eric Auchard & Stephen Neillis, "What is 5G and who are the major players?" Reuters, March 15, 2018, available at: https://www.reuters.com/article/us-qualcomm-m-a-broadcom-5g/what-is-5g-and-who-are-the-major-players-idUSKCN1GR1IN

8. Vindu Goel, "To Keep U.S. Jobs, Chip Makers Share a Factory and Pin Hopes on Trump," *New York Times*, February 26, 2017, available at: https://www.nytimes.com/2017/02/26/technology/im-flash-intel-micron-manufacturing-trump.html

9. *Ibid.* American service providers Verizon, Sprint, T-Mobile and AT&T have set up prototype networks in several American cities. Verizon, Sprint and AT&T are using Ericsson, Nokia and Samsung equipment; T-Mobile uses Ericsson and Nokia.

10. Niclas Rolander & Sam Kim, "Samsung's 5G Network Grab Gets Boost With Huawei, ZTE Under Fire," Bloomberg, December 12, 2019, available at: https://www.bloomberg.com/news/articles/2018-12-19/samsung-s-5g-network-grab-gets-boost-with-huawei-zte-under-fire

With 5G rollouts very much underway, few experts believe any American technology company can put together a comprehensive 5G offering. There is a real need for U.S. companies to find overseas partners. With the exception of Korea, Finland, and Sweden, the same is true of most U.S. free-market partners.

China's Domestic Market Advantage

Even Samsung lacks the clear government 5G mandate that Huawei and ZTE enjoy in the People's Republic of China. As early as its 13th Five Year Plan, the Chinese government identified 5G as a "strategic emerging industry," and later called it a "new area of growth" in its *Made in China 2025* plan. Recognizing that domestic success can translate into a global edge, China is investing heavily in its domestic 5G industry and market.[11] Over 1 billion Chinese use cellular devices, more than the number of users in the United States, Japan, Indonesia, Russia, and Germany combined.[12] The domestic Chinese 5G market is predicted by Chinese experts to reach 428 million users by 2025.[13] The Chinese government aims to support rapid internal 5G development using subsidies, free spectrum allocation, tax breaks, coerced technology transfer, and overseas intellectual property acquisition.[14] For example, the municipal government of Shenzhen has authorized a city-wide 5G development program that will use municipal monies to fund installation of 45,000 5G base stations by 2020 and bear other costs of building out a 5G infrastructure. It will also use its municipal powers to reduce electricity charges for 5G gear and to obtain land-use permission for building base stations and other installations.[15] While other nations have dedicated public funds to develop 5G, nobody has championed development of

---

11. *Ibid.*

12. Bien Perez & Li Tao, "Made in China 2025: How 5G could put China in charge of the wireless backbone and ahead of the pack," *South China Morning Post,* October 16, 2018, available at: https://www.scmp.com/tech/enterprises/article/2168665/made-china-2025-5g-offers-worlds-biggest-mobile-market-chance-seize

13. GSMA Intelligence, "5G in China: Outlook and Regional Comparisons", p.4, 2017, available at: https://www.gsmaintelligence.com/research/?file=67a750f6114580b86045a6a0f9587ea0&download

14. Jamie McBride & Andrew Chatzky, "Is 'Made in China 2025' a Threat to Global Trade?" Council on Foreign Relations, May 13, 2019, available at: https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade;

    Harold Furchtgott-Roth, "Chinese Government Helps Huawei With 5G," *Forbes*, May 8, 2017, available at: https://www.forbes.com/sites/haroldfurchtgottroth/2017/05/08/chinese-government-helps-huawei-with-5g/#4a2db1ab6bae

15. Paul Zhou, "Shenzhen Subsidizes 5G Deployment: Why are Governments around the World Subsidizing 5G?" Telecoms.com Newsletter, September 23, 2019, available at: https://telecoms.com/intelligence/shenzhen-subsidizes-5g-deployment-why-are-governments-around-the-world-subsidizing-5g/

5G at the national and local level on a scale similar to China. Industry sectors like 5G identified in China's national economic plans are also, security experts believe, being supported by an orchestrated effort by state intelligence organs to steal Western technology. This includes traditional espionage involving spies and agents as well as cyber intrusions into Western companies' IT networks to steal trade secrets.[16]

Within this ecosystem of government support, Chinese leaders have directed the largest three telecoms to move forward on 5G and have allocated the optimum spectrum bands to these companies without charge.[17] In addition, they have mandated that Chinese companies be awarded a fixed proportion of all new 5G contracts. This guarantee provides Chinese companies with the revenue and capital to finance very competitive bids for international business. They are busy setting up networks in many large Chinese cities and experimenting with applications. The Chinese government has no intention to allow foreign companies to succeed in scale within the Chinese domestic 5G market. At a minimum, foreign vendors selling into the Chinese market can expect the government to demand that the firm work with local partners and to transfer its technology to them.[18]

Using their protected access to the Chinese market to generate revenue, develop products, and build large-scale network experience, Huawei and ZTE will be uniquely positioned to target export markets in Asia, Europe, and North America with adequate quality, low-cost 5G equipment.

Unfair Competition in Overseas Markets

In their push into overseas markets, many experts believe China's telecom equipment makers, including Huawei, unfairly benefit from both state-sponsored subsidies in violation of WTO[19] as

16. National Counterintelligence and Security Center, "Foreign Economic Espionage in Cyberspace," NCSC, 2018, available at: https://www.hsdl.org/?view&did=813528

17. Li Tao & Bien Perez, "China awards 5G licenses to country's major telecoms network operators, cable network giant," *South China Morning Post*, June 6, 2019, available at: https://www.scmp.com/tech/big-tech/article/3013302/china-awards-5g-licences-countrys-major-telecoms-network-operators

18. Julie Wernau, "Forced Tech Transfers Are on the Rise in China, European Firms Say," *Wall Street Journal*, May 20, 2019, available at: https://www.wsj.com/articles/forced-tech-transfers-are-on-the-rise-in-china-european-firms-say-11558344240;

    Patrick A. Mulloy, "Coerced Tech Transfer: The Heart of the China Problem," *The American Prospect*, June 26, 2019, available at: https://prospect.org/article/coerced-tech-transfer-heart-china-problem

19. Lee Chyen Yee & Simon Johnson, "China's Huawei and ZTE deny getting illegal subsidy," Reuters, May 29, 2012, available at:

well as a concerted effort by state intelligence services to steal the technological secrets of western companies.[20] China's economic "self-help" has been the source of trade friction with the United States and allies, leading to a promise by President Xi to President Obama in 2015 not to target U.S. intellectual property.[21] It appears that if China reduced these operations at all, it was only for a limited time. In July 2019, the FBI announced that it had 1,000 open economic espionage cases in which the perpetrators were acting on behalf of China. FBI Director Cristopher Wray described China's economic espionage as the nation's greatest counterintelligence threat. This economic espionage is a direct threat to free trade, intellectual property protections, and the economic welfare of the citizens of the U.S. and its allies.[22]

It is time for policymakers to recognize that even as China enjoys the benefits the free trade system built by the West, it is willing at the same time to take illegal measures to take advantage of the same system. The system of dispute adjudication that the West had built to handle the infrequent illegal behavior of companies in the like-minded free-trade democracies is not strong enough to handle current Chinese mercantilist practices. The United States, Japan, and other like-minded countries must develop a more aggressive set of measures to counter the advantage that China provides its national champions.

Huawei-specific Instances of Unfair Trade Practices

Huawei has been accused of stealing U.S. cellular technology in a number of cases that date back to 2003:

- 2003 - Huawei admits in U.S. court to stealing router code from Cisco and using it in its competing VRP router software. At trial, Cisco produced evidence of large-scale theft of code, including comments and help screens in which Huawei's text contained identical typos to Cisco code.[23]

---

https://www.reuters.com/article/us-china-huawei-subsidies-idUSBRE85M02U20120623

20. Charles Wallace, "Intelligence Chiefs Back Trump on Chinese Technology Theft," *Forbes*, January 30, 2019, available at: https://www.forbes.com/sites/charleswallace1/2019/01/30/intelligence-chiefs-back-trump-on-chinese-technology-theft/#b90bf3723a0d

21. Editorial Board, "China's Hacking State,"*Wall Street Journal*, December 20, 2018, available at: https://www.wsj.com/articles/chinas-hacking-state-11545353192

22. Robert Delaney, "Chinese tech company Huawei investigated for violating Iran sanctions by US Department of Justice," *South China Morning Post*, April 25, 2018, available at: https://www.scmp.com/news/china/article/2143355/chinese-tech-company-huawei-investigated-violating-iran-sanctions-us

23. Scott Thurm, "Huawei Admits Copying Code from Cisco in Router Software," *Wall Street Journal*, March 24, 2003, available at:

- 2007 - Motorola engineer Hanjuan Jin stopped at O'Hare Airport with a bag filled with sensitive Motorola documents, $30,000 in cash, and a one-way ticket to Beijing. She intended to take a job with a Chinese telecom company, Sun Kaisens.[24]

- 2014 - Huawei engineers visiting a secure T-Mobile facility steal information and a "finger" off of a T-Mobile robot. In 2017, a jury awarded T-Mobile $4.8 million for trade secret misappropriation.[25]

- 2018 – DoJ indicts Huawei for selling sanctioned goods to Iran. At the request of the United States, Canadian authorities arrest the daughter of Huawei's CEO and the company's Chief Financial Officer, Weng Wanzhou, as she transits the Vancouver International Airport. The United States alleges Wanzhou lied to Huawei's lenders as part of a secret scheme by which Huawei acted as a middleman for Iranian purchases of banned U.S. goods.[26]

- 2019 – DoJ indicts Chinese professor at Texas university for stealing trade secrets on behalf of Huawei.[27]

At this point, much of the damage from IP theft is probably already done. Huawei is no longer dependent on stealing technology to build cutting-edge technologies. As well as the assured revenue of protected domestic markets, Huawei has the talent, research funds, academic partners, and acquisition savvy to develop or buy what it needs to compete. Many western telecom manufacturers procure Huawei gear because of its combination of low pricing and adequate quality. However, the final form of international 5G networks has not yet been determined, and based on past behavior, Huawei and ZTE will use any means they can, legal and illegal, to gain a competitive advantage.

---

https://www.wsj.com/articles/SB10485560675556000;

Mark Chandler, "Huawei and Cisco's Source Code: Correcting the Record," Cisco Blogs, October 11, 2012, available at:
https://blogs.cisco.com/news/huawei-and-ciscos-source-code-correcting-the-record

24. Jeff Ferry, "Top Ten Cases of Chinese IP Theft," *Coalition for a Prosperous America*, May 1, 2018, available at: https://www.prosperousamerica.org/top_ten_cases_of_chinese_ip_theft

25. *Ibid.*

26. *Ibid.*

27. Kate O'Keeffe & Aruna Viswanatha, "U.S. Files Criminal Charges Against Chinese Professor Linked to Huawei," *Wall Street Journal*, Sept. 9, 2019, available at: https://www.wsj.com/articles/u-s-files-criminal-charges-against-chinese-professor-linked-to-huawei-11568048700# =

Moreover, the sanctions evasions led by Huawei's CFO and daughter of its founder and current CEO give an insight into Huawei's corporate culture. Major multinationals have generally refrained from transactions that carried reputational risk. That Huawei top leadership had directed the selling of U.S. components to Iran and then attempted to mislead Western banks about their actions suggests that it is very willing to act as an agent of the Chinese government. Indeed, the official protests from Beijing when Wanzhou was arrested in Canada suggest that the Chinese considered Huawei's leadership to enjoy a quasi-diplomatic immunity that placed them beyond the reach of U.S. law.[28]

In conclusion, Huawei's long-time record of participation in sanctions evasion and intellectual property theft demonstrate that it is willing to cooperate closely with the Chinese government in ways that are very different and much more threatening than large international IT companies in the free market democracies.

5G Critical Infrastructure Risk

Beyond the economic threat of Beijing's support, Huawei's close relationship with the Chinese leadership raises a second concern. It represents a national security threat to the West.

As 5G grows, it will become a new form of digital critical infrastructure. It must be secured against attack by a variety of nation-state adversaries and opportunistic exploitation by malicious actors. Foreign government influence with its international IT providers is a new form of systemic risk. Existing critical infrastructure regulations were not designed to handle the possibility of supply chain-based compromise of digital critical infrastructure by a nation state.

In addition, 5G networks, like all forms of digital communications, are susceptible to exploitation by malicious attackers. Security depends on well-written code and alert threat identification and patching.

Huawei-supplied 5G systems present both types of risk. It is subject to China's 2017 National Intelligence Law stating "any organization or citizen shall support, assist and cooperate with the state intelligence work in accordance with the law," adding that the state "protects" any individual and organization that aids it.[29] In addition, Huawei hardware and software consistently contains numerous flaws and vulnerabilities that can be exploited by malicious actors. The UK's technical oversight committee for Huawei reported in March 2019 that the

28. Jane Periez, "Huawei Arrest Tests China's Leaders as Fear and Anger Grip Elite," *New York Times*, Dec. 7, 2018, available at: https://www.nytimes.com/2018/12/07/world/asia/huawei-arrest-china.html

29. Arjun Kharpal, "Huawei says it would never hand data to Chinese government. Experts say it would not have a choice," *CNBC,* March 4, 2019, available at: https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html

company's software had vulnerabilities reflecting failings in "basic engineering competence and cybersecurity hygiene."[30]

RESPONSE TO HUAWEI

The initial American response to Huawei, in 2008-9, was motivated primarily by security rather than economic concerns. Government officials quietly alerted major American companies to the national security risks of Huawei equipment, and several of the large telecoms decided against using Huawei in their 4G networks. In 2012 the House Intelligence Committee issued a public report warning companies against purchasing Huawei equipment due to the security risk. Despite these warnings, about a dozen smaller American wireless service providers, primarily in rural areas, have purchased Huawei equipment for their networks. The equipment was often a third less expensive than that of Nokia and Ericson, and the quality and service were adequate.

Beyond warning American companies against purchasing Huawei systems, the U.S. Government has also given similar warnings to allies and other friendly countries. The intel leaders of Five Eyes (United States, Canada, UK, New Zealand, and Australia) agreed in July 2018 that Huawei specifically represented an espionage threat. Realizing that some countries, UK in particular, already had a sizeable Huawei presence, the group agreed that an outright ban was not a feasible countermeasure to this threat.[31] The Trump Administration has undertaken a government-to-government diplomatic effort to persuade allies around the world not to do business with Huawei. Despite agreement by New Zealand and Australia to ban Huawei from 5G,[32] a number of governments, including the UK, France, Germany, and Italy have publicly stated that they would not do so. Instead, each is moving forward with some form of review mechanism to allow government officials to conduct a risk versus benefit analysis for Huawei-made 5G equipment.[33]

The economic concerns about domination of the 5G industry by Chinese companies has grown with the overall awareness of Chinese mercantilist policies. The publication in 2015 of *Made in*

30. Lily Hay Newman, "Huawei's Problem isn't Chinese Backdoors. It's Buggy Software," *Wired,* March 28, 2019, available at: https://www.wired.com/story/huawei-threat-isnt-backdoors-its-bugs/

30. Tom McKay, "'Five Eyes' Spy Chiefs Agreed to Contain Huawei's Global Reach at Meeting in July: Report," *Gizmodo*, December 16, 2018, available at: https://gizmodo.com/five-eyes-spy-chiefs-agreed-to-contain-huaweis-global-r-183113190

32. Staff, "Tech Giant Huawei banned from New Zealand's 5G network over 'significant' security risks," *South China Morning Post*, Nov. 28, 2018, available at: https://www.scmp.com/news/asia/australasia/article/2175374/tech-giant-huawei-banned-new-zealands-5g-network-over

33. Christoper Scott, "Italy, Germany resist ban on Huawei's 5G gear," *Asia Times*, Feb.7, 2019, available at: https://www.asiatimes.com/2019/02/article/italy-germany-reject-ban-on-huaweis-5g-gear/

China 2025, a blueprint for Chinese domination of the most important technologies of the future, caused intense concern in Western government and business circles. China is now increasingly seen in the United States, Europe, and Japan as an unfair economic competitor, willing to use all tactics, whether compliant with WTO rules tactics or not, to favor Chinese companies in domestic markets, take technology from international companies by any means available, and then encourage Chinese companies to compete abroad. Huawei is perhaps the most successful example of this Chinese approach to domination of an important international industry.

It has been in the last two years, under the current administration, that the United States government has taken the strongest actions to counter Huawei and ZTE, the two Chinese companies that are positioned to be the market leaders in 5G. These specific penalties directed at these two companies take place against the background of the across-the-board tariffs imposed by the United States against imports from China, beginning in July 2018.

In 2018 the U.S. Government effectively put ZTE out of business. Because ZTE had evaded American sanctions on Iran, the government blocked the sale of U.S. chips to the company, without which it could not manufacture its basic equipment. The United States scaled back these sanctions following payment of a large fine and management changes in ZTE.

The U.S. Department of Justice also pursued Huawei for selling sanctioned goods to Iran and attempting to hide its role. The daughter of Huawei's CEO and Chief Financial Officer, Weng Wanzhou, was arrested in Canada in December 2018, at the request of the U.S. Department of Justice. She has been accused of lying to banks as part of a secret scheme by which Huawei acted as a middleman for Iranian purchases of banned U.S. goods.[34] The Justice Department in a separate action has brought a suit against Huawei for stealing trade secrets.

In May of 2019, the U.S. Government issued the Executive Order on Securing the Information and Communications Technology and Services Supply Chain" ("Executive Order on Communications Technology")[35] and followed it with Commerce Department action to add Huawei and its affiliates to the Export Administration Regulations' sanctioned Entity List maintained by the Bureau of Industry and Security ("Huawei ban").[36]

---

34. *Ibid.*

35. President Donald J. Trump, "Executive Order on Securing the Information and Communications Technology and Services Supply Chain," White House, May 15, 2019, available at: https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/

36. Bureau of Industry and Security, "Addition of Certain Entities to the Entity List (final rule), effective May 16, 2019," available at:

Most recently, in July 2019, the FBI announced that it had 1,000 open economic espionage cases in which the perpetrators were acting on behalf of China. FBI Director Cristopher Wray described China's economic espionage as the nation's greatest counterintelligence threat. China's economic espionage was described as a direct threat to free trade, intellectual property protections, and the economic welfare of the citizens of the United States and its allies.[37] DoJ also brought a criminal action against a Chinese professor in Texas who is accused of misappropriating research on behalf of Huawei.[38]

Net Assessment of the Response to Huawei

The advantage of the current U.S. approach of using sanctions evasion authorities to deal with ZTE and Huawei is that penalties are swift, significant, and flexible. Traditional remedies such as WTO cases, anti-dumping actions, federal fraud statutes, and copyright and patent infringement cases, on the other hand, unfold too slowly to deter foreign companies from predatory actions or protect U.S. companies from substantial losses. By the time a verdict is reached, the damage is done. The case of Sinovel's theft of the American company AMSC's computer code for operating windmills provides a clear example. The suit was brought by AMSC in 2013, but not settled until 2018. AMSC was paid about $50 million for losses that exceeded $800 million. Under the existing system, the onus is on the victim to invest the funds necessary to building a case and losses mount while the plaintiff waits for a verdict. Too often, this means that the plaintiff is bankrupt by the time a final decision is rendered.

The weakness in the U.S. approach to Huawei and ZTE has been focusing on the national security risk of ZTE and Huawei's behavior, but not countering the consequences of these same state-supported predatory practices for private sector firms in the West. The United States has used the heavy penalties against ZTE and Huawei for sanctions evasion and warnings to other countries about national security risks as a way both to keep these companies out of the U.S. market and to hinder its worldwide expansion. At the same time, nothing has been done to

---

https://www.bis.doc.gov/index.php/all-articles/17-regulations/1555-addition-of-certain-entities-to-the-entity-list-final-rule-effective-may-16-2019;

Announcement in Federal Register found here:
https://www.bis.doc.gov/index.php/documents/regulations-docs/2394-huawei-and-affiliates-entity-list-rule/file

37. Robert Delaney, "Chinese tech company Huawei investigated for violating Iran sanctions by US Department of Justice," *South China Morning Post,* April 25, 2018, available at: https://www.scmp.com/news/china/article/2143355/chinese-tech-company-huawei-investigated-violating-iran-sanctions-us

38. Kate O'Keeffe & Aruna Viswanatha, "U.S. Files Criminal Charges Against Chinese Professor Linked to Huawei," *Wall Street Journal*, September 9, 2019, available at: https://www.wsj.com/articles/u-s-files-criminal-charges-against-chinese-professor-linked-to-huawei-11568048700# =

help Western competitors whose intellectual property and market share is at risk. The Commission recommends that the United States develop a new complaint system for victims of predatory practices from known bad actors that immediately protects a U.S. firm that petitions for relief from the bad actor's wrongful actions and shifts the burden of proof to the known bad actors to prove their behavior is not harmful. The Commission also believes that the pervasive evidence of state involvement in Chinese companies' predatory practices justifies financing and other assistance to help firms operating in strategic sectors subject to these practices.

Over the long term, however, the legal basis and the actions to deal with the economic threat due to orchestrated Chinese support for its national champion companies should be separated from the legal basis and actions to deal with the national security threat of integrating Chinese components into 5G networks. The risk of integrating Chinese-made equipment is only one example (albeit the most serious) of the systemic risk to digital critical infrastructure of using equipment that might be compromised by a hostile government. Only by distinguishing between these two different threats and taking appropriate actions to deal with them will the United States be able to build international cooperation from its allies, friends, and other important countries such as India and Indonesia. The current approach forces them to choose sides between the United States and China, rather than requesting them to uphold international norms and standards.

In addition, clarifying and aligning the objectives and actions provides a basis for reaching an ultimate agreement with China through discrete steps. If China eliminates its unfair subsidies, then the United States can reduce its penalties against Chinese companies that benefit from them. If Huawei can demonstrate that it is independent of Chinese government influence, then 5G market access can be revisited.

A second problem with the current ban on Huawei is that it is too broad. It disrupts too many profitable business relationships and threatens the economic welfare of some of the same U.S. firms that are best positioned to compete within the 5G market. Specifically:

- It denies lucrative sales of U.S.-made and U.S.-designed chips and components to Huawei, reducing profits that could be used for 5G development.[39]

- It incentivizes Huawei to develop alternative suppliers and alternative technologies for its gear, a process which in the long term means that the U.S. suppliers lose a valuable customer even if sanctions are rescinded.[40]

---

39. Frank Bajak & Michael Liedtke, "Huawei sanctions: Who gets hurt in the dispute?," *USA Today*, May 21, 2019, available at: https://www.usatoday.com/story/tech/news/2019/05/21/huawei-why-facing-sanctions-and-who-get-hurt-most/3750738002/

40. Cameron Faulkner, "Can Huawei make a phone without US parts?," The Verge, May 21, 2019, available at:

- It creates havoc for existing customers of Huawei, particularly rural cellular service providers even though these customers are not 5G network operators.[41]

- It blocks Google from pushing security updates to owners of Huawei smartphones (who are outside the scope of the ban) because the updates must go through Huawei.[42]

- It thereby incentivizes Huawei to develop a replacement for Android, which, if successful, would be another significant market loss for US suppliers.[43]

RECOMMENDATIONS

In light of the issues and challenges outlined above, the Commission recommends the following actions:

ESTABLISH A TWO-PRONGED REVIEW FOR PROCUREMENT OF FOREIGN-MADE 5G EQUIPMENT

Integration of Huawei equipment onto 5G networks carries with it two risks: (1) risk that Huawei will allow the Chinese government to use its initial installation or maintenance tools to access the network for nefarious purposes and (2) the possibility that sloppy engineering will leave the gear vulnerable to compromise by opportunistic hackers.

The first risk applies uniquely to China and other adversaries at odds with the United States and free-market democracies. Finland and Sweden, home countries for Nokia and Ericson, do not pose this risk. The second risk applies to all foreign-supplied hardware and software in 5G systems. The two-prong approach reflects the fact that the two types of risk are different in character and require a review involving fundamentally different data, criteria, and expertise.

https://www.theverge.com/2019/5/21/18632550/huawei-p30-pro-android-google-executive-order-us-phone-qualcomm-intel

41. BBC Wires, "Huawei Equipment Ban Could Disrupts [sic] Rural Telecom Operators," *BroadbandCommunities*, July 1, 2019, available at: https://www.bbcmag.com/breaking-news/huawei-equipment-ban-could-disrupts-rural-telecom-operators

42. Jay McGregor, "Here's How Huawei's Android Ban Affects You [Updated]," *Forbes*, May 20, 2019, available at: https://www.forbes.com/sites/jaymcgregor/2019/05/20/huawei-android-ban-what-it-means-for-your-phone/#56d687d761b1

43. David Phelan, "Move Over Android: Huawei's Harmony OS is Plan B, But Could Be Implemented 'In Days' If Needed," *Forbes*, August 10, 2019, available at: https://www.forbes.com/sites/davidphelan/2019/08/10/move-over-android-huaweis-harmony-os-is-plan-b-but-could-be-implemented-in-days-if-needed/

Susceptibility to Manipulation by a Foreign Government

The risk of foreign government pressure on a 5G equipment supplier is a political judgement based on advice from foreign policy, economic, and intelligence agencies, along with private sector input. In the United States, these risks are routinely evaluated by the Committee on Foreign Investment in the United States ("CFIUS"), led by the Treasury Department, which reviews foreign investments in American companies in the security sector. It makes sense for the United States to use this same set of government officials to review relationships between foreign 5G equipment suppliers and their host government. The process for 5G equipment review, however, is more logically led by the Secretary of Commerce because the President's executive order on foreign influence in telecommunications equipment appoints the Secretary of Commerce to lead this effort.

Other countries have their own, sometimes *ad hoc*, processes for approving the purchase of telecommunications equipment from foreign suppliers. The Commission recommends that they similarly institutionalize the review of foreign-made 5G equipment procurement to ensure such review continues over the extended period of time that it will take to roll out 5G networks.

Assessing Technical Vulnerabilities

Assessing the risk of introducing vulnerable foreign equipment into a 5G network is another process that countries must institutionalize, but this is primarily a technical process, requiring exhaustive examination of computer code and the design and operation of hardware. The only free-market democracy that has set up a government organization to perform this function is the United Kingdom, which formed the Huawei Cyber Security Evaluation Centre ("HCSEC"). The reports of the HCSEC have been extremely valuable in guiding UK decisions on Huawei and informing discussion of the issue in other countries. The Commission recommends that similar organizations be set up in other countries, led by technically competent government engineers and qualified personnel. Such organizations must be able to tap talent from the private sector and academia when their relevant expertise is required.

Where feasible, if a technical review committee finds a deficiency, it should recommend improvements or mitigations that the foreign supplier or purchasing telecom carrier can make to meet security standards. Otherwise, if equipment risks cannot be sufficiently controlled, procurement of the equipment should be prohibited. Reviews of foreign-made 5G equipment should be a continuing processes as new models are developed, and new technology incorporated. It also may require some form of equipment monitoring by the telecom or the government to ensure security is not compromised later through patches or other upgrades.

The Commission recommends that both the political risk committees and the technical risk committees in the free market democratic countries cooperate closely via the "5G International Security Council" recommended below. While every country will want its own policymakers and technical experts to make the final decisions on what is permitted to be integrated into its 5G

infrastructure, all should take advantage of the work done by allies in addressing the same risks and the same suppliers.

Commission Recommendation:

1. Establish a two-prong domestic review mechanism to review 5G network procurement from foreign suppliers to ensure that telecom carriers purchase equipment (1) not at high risk of compromise through pressure on the supplier by an unfriendly government and (2) built with sufficient security features to minimize the risk for opportunistic hackers to compromise the gear.

    a. For the United States:

        i. Direct the recently reformed Committee on Foreign Investment in the U.S. ("CFIUS"), under the leadership of the Secretary of Commerce, to screen all foreign 5G equipment providers.

        ii. Establish a government cybersecurity evaluation center to conduct technical audits of the hardware and software of foreign 5G suppliers for high security standards.

    b. For Japan:

        i. Direct the Ministry of Trade, the Economy and Industry (METI) to lead an interdepartmental process for screening foreign 5G equipment providers for political risk.

        ii. Direct the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) to lead technical audits of foreign-supplied 5G equipment for high security standards.

    c. For like-minded European countries: Establish or formalize analogous bodies and processes to assess risk and allow the purchase of foreign 5G systems.

STRENGTHEN POLICIES TO IDENTIFY AND PENALIZE FOREIGN FIRMS WITH UNFAIR GOVERNMENT SUPPORT

There is ample evidence of China engaging in illicit activities through and for its industry, but existing efforts to counter China's unfair trade practices bog down in the heavily evidence-based adjudication systems invoked in tariff disputes and criminal investigations. Legislation already exists in the United States that would allow the Executive Branch to implement an accelerated process that shifts the burden of proof to foreign companies conducting or benefiting from illegal activities.

The President should use executive authority under the International Trade Commission 337 process, the International Emergency Economic Powers Act (IEEPA), and the 2015 National Defense Authorization Act, Section 1637 to implement an accelerated process to impose

penalties on foreign firms. Under this process, a designated government official would make speedy decisions on the validity of complaints from American companies of illegal competition from foreign companies. The designated official would then, depending on the nature and extent of the case, impose penalties including fines, revocation of import licenses, withdrawal of permission to use U.S. components, restriction of the use of the U.S. banking system, and other measures. It would then be up to the penalized foreign company to produce the evidence and information to rebut the presumption of wrongdoing and regain its access to U.S. markets and partners.

The Commission recommends that the U.S. implement such a process to protect its 5G companies from unfair Chinese competition. This tool could be used in tandem with current tariff and criminal proceedings, and would help ensure that victims of unfair trade practices are not pushed into bankruptcy waiting for a verdict. Free-market democracies have won many WTO cases against Chinese companies and prevailed in litigation over theft of trade secrets. Unfortunately, these successes have neither caused China to reform its mercantilist policies nor stemmed the illicit flow of intellectual property. The only way to fix this is to shift the costs of China's illegal activity from the victims to the perpetrators while the appeal process proceeds.

Japan and like-minded countries in Europe and elsewhere can establish similar procedures, and all countries can coordinate these actions within the 5G International Security Council. These procedures will in the near term ensure that Western 5G companies do not face unfair competition, and in the long term provide a basis for negotiations with China to change its mercantilist policies.

Commission Recommendation:

1. Strengthen domestic policies and actions to penalize foreign firms supplying 5G equipment that benefit from predatory support from their governments or conduct illegal activities such as IP theft. Establish a process for rapid government decisions and imposition of penalties by experienced officials, shifting the burden of proof from the domestic victim to the foreign supplier. Tailor penalties for specific companies to the scale of economic damage.

    a. For the United States: Interpret or improve existing authorities to establish a rapid process to penalize subsidies and illegal behavior by foreign companies and to shift the burden of proof from victim companies. Existing legislation includes the International Trade Commission 337 process, the International Emergency Economic Powers Act (IEEPA), and the 2015 National Defense Authorization Act, Section 1637.

    b. For Japan: Establish an administrative process led by the Ministry of Economy, Trade and Industry that will provide speedy decisions to penalize foreign suppliers of 5G equipment benefitting from illegal government support or illegal activities.

c. For like-minded European countries: Set up analogous procedures using appropriate government official.

PROMOTE LOCAL 5G VENDORS AND JOINT VENTURES IN THE INTERESTS OF NATIONAL SECURITY

The United States and many of its allies host firms that own intellectual property of enormous value to the 5G community, but most do not possess a single firm capable of manufacturing and integrating an entire 5G network. In fact, in the case of the United States, UK, Japan, Germany, Italy, and France, large portions of the 5G network must be built using foreign-made equipment. For a variety of reasons, IT sector developments in these countries have not produced major companies that can provide end-to-end 5G solutions. A trade policy that only shuts Chinese companies out, but does not encourage the development of alternative suppliers, is not sustainable. China's illicit support to its high-tech players, however, justifies industrial policy that promotes and nurture 5G companies in the free market democracies.

Normally, incentives or subsidies to 5G firms would be a violation of WTO rules, but China's actions justify exercising the national security exception to WTO rules contained in Article XXI of the General Agreement on Trade and Tariffs.[44] In other words, the United States and its allies should develop a series of domestic industry promotion and cross-border investment incentives to help local firms team with other Western firms to develop 5G products and markets. The governments would handle any objections by China or other nations under WTO by invoking Article XXI, which states:

> *Nothing in this Agreement shall be construed . . . (b) to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security interests . . . .*[45]

There are a number of challenges facing 5G rollouts that could be tackled now if companies could secure the funding. Optimal spectrum allocation is one example. This task is more difficult for advanced economies with complicated, pre-existing spectrum allocation schemes. For example, in the United States, the Department of Defense has sole rights to a large amount of sub-6 GHz spectrum that is optimal for 5G network coverage. The U.S. government is looking at ways to not only re-apportion this bandwidth, but to share it. The latter option, in turn, asks for a technical solution such as band hopping to facilitate simultaneous use of bandwidth by multiple parties. Companies that develop this sort of solution would find potential customers around the world facing similar needs to share spectrum. Government funding that

---

44. See William A. Reinsch & Jack Caporal, "The WTO's First Ruling on National Security: What Does It Mean for the United States," Center for Strategic and International Studies, April 4, 2019, available at: https://www.csis.org/analysis/wtos-first-ruling-national-security-what-does-it-mean-united-states

45. World Trade Organization, "General Agreement on Tariffs and Trade," 1994, Article XXI, available at: https://www.wto.org/english/docs_e/legal_e/06-gatt_e.htm

spearheaded development of such solutions would directly contribute to developing a local 5G industry capable of pursuing global markets. Similar opportunities exist for governments to fund research into technical solutions to carry secure 5G communications over untrusted network segments, disaster redundancy for 5G and 5G-dependent technologies, and security research around defining and protecting "high risk" elements of the 5G network. Creating an open and vendor-agnostic communications protocol that allows 5G networks from all suppliers to communicate with existing 3G and 4G networks would lower the cost of integrating equipment from new vendors that needs to communicate with telecom carriers' substantial existing infrastructure. This would reduce the risk of "vendor lock-in" and open up 5G markets to wider competition. A related area of research would be open standards for modular 5G architecture that partition 5G networks into segments that speak to each other using open protocols. Again, this would facilitate competition by allowing telecoms to purchase equipment built to open specifications from a wider community of developers. Funding these initiatives would help jumpstart local 5G industry and promote development of alternatives to a 5G sector dominated by China.

For the United States, 5G industrial policy must include consideration of tax incentives to assist firms (including firms from like-minded democracies) in investing in 5G research and businesses. It also might require anti-trust waivers such as were instituted under the Cybersecurity Information Sharing Act of 2016 to permit 5G partnerships. Finally, research funding to help firms establish open protocols and standards that will shape the applications and communications that run on 5G will be of direct benefit in developing a 5G cottage industry and offset some of the first-to-market advantages that China's national champions are poised to grab.

Furthermore, development of large full-service 5G competitors to Huawei cannot happen without international collaboration among vendors. Thus, it is crucial that domestic recommendations be implemented in a way that encourages *cross-border* collaboration.

Partnerships with overseas partners could take one of many forms. Building alliances among U.S., Japanese, and European firms to develop a new 5G end-to-end network for international sale is one possibility. Attracting one of the established vendors from a trusted US ally (Samsung, Ericsson, or Nokia) to set up major operations in the United States might be, for the U.S., another. Creating the incentives and market conditions for promoting these cross-border partnerships must be part of any national 5G security and economic policies implemented by the United States and its allies. Without such concerted action, the outcome is likely a global 5G market dominated by China's national champions.[46]

46. Granted, there are few examples of public sector-led industrial collaboration—Airbus and the Joint Strike Fighter program come to mind—and mixed views on the efficacy of this approach. Even so, without trying to duplicate China's mercantilist approach, Western nations must encourage their 5G vendors to work together in

Commission Recommendations:

1. Promote the development of a robust, open domestic 5G sector in the free market democracies capable of building alternative 5G solutions

    a. Support open protocols to enable 5G gear to intercommunicate with 3G and 4G networks in order to reduce "vendor lock-in" and the resulting the barrier to entry for new 5G firms.

    b. Support an open and modular architecture for 5G networks that permits carriers to integrate equipment from various sources without significant integration costs.

    c. Create investment incentives designed to encourage domestic companies and overseas firms from trusted nations to invest in 5G technologies and networks.

    d. Encourage industry cooperation in forming 5G system suppliers by the selective use of waivers to federal and state antitrust law as was done in the United States with the Cybersecurity Information Sharing Act of 2016.

    e. Incentivize participation in domestic 5G system ventures to qualified foreign firms from trusted allies.

2. Fund basic research in critical 5G technology not taking place in the private sector. Examples include:

    a. Improved technology for spectrum sharing in the prime 5G frequency bands.

    b. Secure communications over untrusted networks.

    c. Identification and segregation of "high risk" components in 5G networks for which foreign components carrying high political risk should never be used, and "low risk" components subject to lower security requirements.

5G International Security Council ("5G ISC")

Finally, the Commission recommend that the United States and its allies and other democratic free market countries form a council, the 5G ISC, to handle the international coordination necessary to carry out our other recommendations. The 5G ISC would act as a joint task force for investigating incidents of Chinese and other government/private sector collusion as well as assist member states in building a case for action. It would also facilitate harmonization of national security and technical review of foreign-made equipment to simplify the process and

order to develop competitive 5G alternatives and an effective way to do this is to make qualified foreign partners eligible to participate in domestic promotion schemes.

possibly permit cross-accreditation. Finally, it could help firms and regulators find cross-border solutions and partnerships to build robust 5G alternatives.

Commission Recommendation:

1. Establish a "5G International Security Council" as the primary mechanism for international coordination of 5G security and trade policies of the member states. The council would include government officials with national security, economic and digital infrastructure regulation responsibilities, as well as representatives from major 5G providers and vendors. The 5G ISC would have the following responsibilities:

    A. Coordination of the criteria to be used for each member country's review of the political risk of foreign 5G equipment suppliers, along with comparison and potential coordination of specific results of reviews.

    B. Coordination of technical standards used to assess the security risk of 5G vendor hardware and software, along with comparison and potential coordination of specific results of reviews.

    C. Continuous sharing of threat and risk assessments among the council members.

    D. Coordination on spectrum allocation issues.

    E. Developing and coordinating opportunities for partnerships among member nation's companies to facilitate development of robust, price-competitive alternatives to Huawei and ZTE while ensuring any antitrust or trade treaty concerns are preemptively addressed

    F. Coordination of research into new technologies for spectrum sharing, secure end-to-end communications over future 5G networks for specific organizations.

    G. Comparison of technical reviews and agreement on "high" vs. "low" risk components of 5G networks.

* * *

APPENDIX A: TIMELINE OF WESTERN SECURITY-RELATED ACTIONS AGAINST HUAWEI

July 2018

3. Five Eyes intelligence officials meet to discuss Huawei in Canada. They conclude the company represents a significant threat to the West, but due to UK carriers' reliance on Huawei equipment they refrain from calling for an outright ban.[47]

August 2018

4. Australia bans Huawei and ZTE from future 5G networks while Signals Directorate Director-General Mike Burgess publicly advocates the need to ban Huawei.[48]

5. President Trump signs a law banning federal agencies and contractors from using Huawei and ZTE gear. U.S. officials quietly starts lobbying Japan, Italy, and Germany to ban Huawei as well.[49]

November 2018

- New Zealand bans its largest mobile carrier, Spark, from procuring Huawei 5G equipment.[50]

---

47. Chris Uhlmann & Angus Grigg, "Secret meeting led to the international effort to stop China's cyber espionage," *Financial Review*, December 13, 2018, available at: https://www.afr.com/world/asia/secret-meeting-led-to-the-international-effort-to-stop-chinas-cyber-espionage-20181213-h192ky

48. Gareth Hutchens, "Huawei poses security threat to Australia's infrastructure," *The Guardian*, October 29, 2018, available at: https://www.theguardian.com/australia-news/2018/oct/30/huawei-poses-security-threat-to-australias-infrastructure-spy-chief-says;

    Christopher Knaus, "Marise Payne defends 5G ban on Chinese telcos Huawei and ZTE," *The Guardian*, August 27, 2018, available at: https://www.theguardian.com/australia-news/2018/aug/27/marise-payne-defends-5g-ban-on-chinese-telcos-huawei-and-zte

49. Jacob Kastrenakes, "Trump signs bill banning government use of Huawei and ZTE tech," *The Verge*, August 13, 2018, available at: https://www.theverge.com/2018/8/13/17686310/huawei-zte-us-government-contractor-ban-trump

    Jon Porter, "The US Government is reportedly trying to persuade allies to stop using Huawei equipment," *The Verge*, November 23, 2018, available at: https://www.theverge.com/2018/11/23/18108649/us-government-huawei-ban-allies-use-subsidies

50. Jasper Jolly, "New Zealand blocks Huawei imports over 'significant security risk,'" *The Guardian*, November 28, 2018, available at:

December 2018

6. British Telecom omits Huawei from list of equipment suppliers for 5G and announces plans to phase Huawei equipment out from its 3G and 4G networks, prompting Huawei to meet with UK's National Cyber Security Centre to work out measures to allow Huawei to compete in UK.[51]

7. Canada, which has not publicly announced plans to ban Huawei from 5G networks, angers China by arresting Huawei CFO Sabrina Meng Wanzhou, for extradition to the United States on charges of circumventing U.S. sanctions on Iran.[52]

8. Japanese government revising procurement rules to make it impossible to purchase Huawei and ZTE equipment while Softbank, NTT DoCoMo, and KDDI as well as future cellular carrier, Rakuten, announce plans to not use Huawei equipment in their future 5G networks.[53]

9. Largest cellular carrier in France, Orange, announces plans to drop Huawei from its 5G network procurement as France's telecom regulator puts Huawei on its "high alert" list.[54]

---

https://www.theguardian.com/business/2018/nov/28/new-zealand-blocks-huawei-5g-equipment-on-security-concerns

51. Staff, "British telecoms giant BT Group to strip Huawei from core networks, limit 5G access," *South China Mornng Post*, December 6, 2018, available at: https://www.scmp.com/tech/gear/article/2176573/british-telecoms-giant-bt-group-strip-huawei-core-networks-limit-5g-access;

    Staff, "Huawei agrees to UK security steps to avoid 5G ban: report," *South China Morning Post*, December 7, 2018, available at: https://www.scmp.com/tech/gear/article/2176968/huawei-agrees-uk-security-steps-avoid-5g-ban-report

52. Rebecca Joseph & Andrew Russell, "Who has taken action against telecom giant Huawei and why Canada hasn't," *Global News*, December 6, 2018, available at: https://globalnews.ca/news/4736209/whos-taken-action-against-huawei-and-why-hasnt-canada/

53. Staff, "Japan to ban Huawei, ZTE from govt contracts-Yomiuri,"Reuters, December 6, 2018, available at: https://www.reuters.com/article/japan-china-huawei/japan-to-ban-huawei-zte-from-govt-contracts-yomiuri-idUSL4N1YB6JJ;

    Minoru Satake, "Japan's 4 carriers to shun Chinese 5G tech," *Nikkei Asian Review*, December 11, 2018, available at: https://asia.nikkei.com/Business/Companies/Japan-s-4-carriers-to-shun-Chinese-5G-tech

54. Staff, "Huawei facing fresh set of problems in France and Germany," Reuters, December 14, 2018, available at: https://telecom.economictimes.indiatimes.com/news/huawei-facing-fresh-set-of-problems-in-france-and-germany/67094312;

10. Germany's Deutsche Telekom announces decision to review its use of Huawei 5G equipment in light of security concerns.[55]

January 2019

11. United States charges Huawei and its Chief Financial Officer, Meng Wanzhou, with evading U.S. sanctions against Iran.[56]

12. United States charges Huawei with 10 counts of industrial espionage.

March 2019

13. UK oversight review board issues sharp criticism for Huawei's failure to fix significant security vulnerabilities in equipment integrated into UK's existing cellular infrastructure, noting that unneeded complexity and human error made existing systems insecure and adding that UK experts were frustrated with Huawei's inability to fix known problems.[57]

May 2019

14. France, Germany, and the Netherlands confirm they will not impose blanket bans on use of Huawei gear on their 5G networks.[58]

Bloomberg, "Huawei faces further woes – in France," *The Straights Times*, December 15, 2018, available at: https://www.straitstimes.com/world/europe/huawei-faces-further-woes-in-france

55. Staff, "Huawei facing fresh set of problems in France and Germany," Reuters, December 14, 2018, available at: https://telecom.economictimes.indiatimes.com/news/huawei-facing-fresh-set-of-problems-in-france-and-germany/67094312

56. David E. Sanger et al, "Huawei and Top Executive Face Criminal Charges in the US," *New York Times*, January 28, 2019, available at: https://www.nytimes.com/2019/01/28/us/politics/meng-wanzhou-huawei-iran.html

57. Jack Stubbs & Cassell Bryan-Low, "Britain rebukes Huawei over security failings, discloses more flaws," Reuters, March 28, 2019, available at: https://www.reuters.com/article/us-huawei-security-britain/britain-rebukes-huawei-over-security-failings-discloses-more-flaws-idUSKCN1R90ZC

58. Staff, "The Latest: Germans, Dutch won't ban Huawei despite US move," AP News, May 16, 2019, available at: https://www.apnews.com/5f4ea81833294d9ab3e92898d0dd51e0

15. Trump Administration issues an executive order[59] authorizing the Commerce Department to ban U.S. firms from doing business with telecom companies whose equipment, if integrated into U.S. networks, constitutes a national security threat.[60]

16. Commerce Department immediate issues a ban on all U.S. firms from dealing with Huawei, citing its intellectual property theft and unfair trade practices as part of its justification for the ban.[61]

17. Commerce immediately delays start date of ban to August amid uproar by companies such as Qualcomm, Google, and UK-based ARM who sell components and chips to Huawei and, in the case of Google, provide Android security updates thru Huawei to Huawei smartphone owners.[62]

June 2019

18. At Osaka G-20 Summit, President Trump assures President Xi that the United States will grant licenses to U.S. firms supplying critical components to Huawei.

July 2019

19. Commerce Secretary Wilbur Ross encourages U.S. firms to seek licenses to do business with Huawei[63]

---

59. President Donald Trump, "Executive Order on Securing the Information and Communications Technology and Services Supply Chain," White House, May 15, 2019, available at: https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/

60. Catalin Cimpanu, "Trump signs executive order banning US telcos from buying or using foreign gear," ZDNet, May 15, 2019, available at: https://www.zdnet.com/article/trump-signs-executive-order-banning-us-telcos-from-buying-or-using-foreign-gear/

61. Bureau of Industry and Security, Department of Commerce, "Addition of Entities to the Entity List," *Federal Register*, May 21, 2019, available at: https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list

62. Ivan Mehta, "Trump Delays Huawei ban by 90 Days,", TNW, May 21, 2019, available at: https://thenextweb.com/tech/2019/05/21/trump-delays-huawei-ban-by-90-days/

63. Dan Strumpf, "Ross Spells Out Reprieve for Huawei," *Wall Street Journal*, updated July 9, 2019, available at: https://www.wsj.com/articles/ross-spells-out-reprieve-for-huawei-11562695409

APPENDIX B – ADDITIONAL ITEMS FOR COLLABORATION

The main body of this report identifies areas in which Western nations should fund research. Generally speaking, these areas are either key to future security or critical to effective spectrum allocation (or both). This appendix elaborates on three of these areas:

- High and low risk areas of 5G networks
- Spectrum allocation and sharing
- Securing communications across untrusted networks
- Open protocols to standardize communication between 5G and legacy 3G/4G systems
- Modular architecture for 5G systems that specify open standards for inter-modular 5G communications

HIGH AND LOW RISK AREAS OF 5G NETWORKS

5G networks are still in the prototype stage and implementations of its standards are still evolving. It is clear, however, that architectural difference with earlier cellular standards will require rethinking fundamental security concepts. The key example of this is "core" and "non-core" functionality. In 4G and earlier systems, most critical functions are handled at the cellular network core. In 5G, to maintain low latency, some services such as message routing and storage, are pushed out to the to the edge, perhaps as far as individual cell towers. This creates a technical challenge as to whether 5G systems can be divided, for security purposes, into "core" and "non-core" components. If this established paradigm for cellular network security does not apply to 5G architectures, the concept of "core" and "non-core" must either be jettisoned or refined to fit with the technical realities of 5G. This is a critical prerequisite to regulators issuing security requirements for 5G. It may be that a new definition of "high risk" and "low risk" components of 5G is required.

Reports of technical disagreements over what requires protection have emerged among government experts from different countries.[64] The United States, Japan, and like-minded European companies must resolve this issue through cooperative technical consultations, to reach a common definition of high and low risk areas of 5G networks. Ultimately, it is the responsibility of each government to fund or conduct the technical research work to determine whether some foreign-supplied components of a 5G network pose no risk. The international 5G

64. Staff, "Explainer: Securing the 5G future – what's the issue?" Reuters, April 24, 2019, available at: https://uk.reuters.com/article/uk-britain-huawei-explainer/explainer-securing-the-5g-future-whats-the-issue-idUKKCN1S01ML

consultative organization recommended later in this report is an appropriate forum for governments to compare their findings and agree on international standards.

Spectrum Allocation and Sharing

5G network providers must have access to sufficient bandwidth to deploy initial networks that will influence 5G standards and provide a foundation for future rapid expansion. The 5G specification allows for network providers to transmit over millimeter wave spectrum ("mmwave") (30-300GHz) or Sub-6GHz spectrum ("Sub-6") (6GHz and below). Although mmwave provides the fastest, highest volume transmissions, its very short wavelength means that it has very poor coverage and is easily blocked by walls, furniture, vehicles, and even human bodies. Building a city-wide mmwave 5G network would require a massive infrastructure rollout that would be extremely expensive and time consuming, and it still would likely suffer from spotty coverage. For this reason, many experts conclude that mmwave 5G will be best used for enterprise-specific base- or plant-wide networks. Meanwhile, Sub-6 uses a frequency that is fast enough to deliver 5G quality speed and latency on a larger scale. With enough bandwidth, it can deliver the required throughput as well. This is the spectrum of choice for building commercial 5G cellular networks.

One challenge in the United States for allocating Sub-6 bandwidth is that large portions of this spectrum have been licensed to the Department of Defense for military communications. DoD, the FCC, and federal partners are scrutinizing these allocations to find bandwidth that can be released and auctioned to 5G vendors. These same parties and a number of commercial firms are also looking at ways to share 5G spectrum using channel hopping and other protocols to share bandwidth dynamically.[65]

Both the issues of which spectrum future 5G networks use (mmwave vs. Sub-6) and how 5G networks share bandwidth with other users, are technical applications that are currently under investigation. As stated earlier, China made clear bands in both frequency ranges available to its telecom companies, with the goal of speeding development and capturing future standards. Spectrum allocation decisions are more complicated outside China. In the United States, the FCC, NTIA, DoD, and other government agencies are in active discussions with 5G developers and service providers to work out allocations that will provide 5G development opportunities, while preserving the services of current frequency users. [66]

65. E.g., Qualcomm, "Spectrum sharing provides critical benefits for 5G," as of November 12, 2019, available at: https://www.qualcomm.com/invention/5g/5g-unlicensed-shared-spectrum

66. The US Defense Innovation Board (an advisory body to the Department of Defense) recommended in April 2019 that the Department of Defense work with other government agencies to give up enough sub-6 bandwidth to allow US operators to develop robust 5G networks within this spectrum. See "Defense Innovation Board, The 5G Ecosystem: Risks & Opportunities for DoD (April 2019)", p.27.

It is critical that national governments and telecom regulators allocate sufficient bands at the correct frequencies if their domestic carriers if they wish to have any hope of competing against China. There is also potential for governments to fund spectrum-sharing research to develop solutions that are competitively marketed in other parts of the world where sub-6 spectrum is already used, giving Western competitors a marketing advantage over 5G implementations that rely on monopolizing large swathes of sub-6 spectrum.

SECURING COMMUNICATIONS ACROSS UNTRUSTED NETWORKS

A number of governments, including the UK, France, Germany, and Italy have publicly stated that they will not implement a complete ban on Huawei sales.[67] Instead, each is moving forward with some form of review mechanism to allow government officials to conduct a risk versus benefit analysis for Huawei-made 5G equipment.[68] This will result in some untrustworthy foreign equipment in future 5G networks in these countries, and many others. This means that no matter how secure a nation's domestic network is, communications, including sensitive ones, must travel across borders and over untrusted networks.[69]

It should be noted that sensitive or critical communications in the 5G world will not be restricted to government and military communications, but include critical data sessions between autonomous vehicles and road sensors, nodes involved in supply chain or manufacturing operations, and data exchange with health monitoring devices that must function to keep patients alive. The providers of these services will have the responsibility to ensure that the devices themselves and the applications that control them are built to high security standards. However, to ensure that the 5G networks over which these services communicate also have the highest security, new concepts and applications, if not new technology, are needed.

The United States, Japan, and like-minded nations must sponsor research and development to invent—if not new technology—new applications of existing authentication, validation, and encryption mechanisms to protect critical communications traveling over 5G networks that include components from Chinese or other untrusted vendors. These solutions must be able to protect not only traditional cellular communications but new forms of data exchange not possible before.[70]

---

67. See Appendix A to this document for a timeline of national security-related actions involving Huawei.

68. See Gemalto, "Five Things that are changing with security in 5G mobile networks," *Gemalto*, September 30, 2019, available at: https://blog.gemalto.com/iot/2016/09/30/five-things-that-are-changing-with-security-in-5g-mobile-networks/

69. *Ibid.*

70. Ericsson, "A guide to 5G Network Security – Executive Summary," Ericsson, as of Aug. 11, 2019, available at:

APPENDIX C – IMPLEMENTING COMMISSION RECOMMENDATIONS IN THE U.S.

The challenge for technical review of 5G networks is that most nations do not conduct any systematic review of equipment integrated into critical telecommunications networks. The one exception is the UK, which has a governmental body that reviews Huawei equipment destined for British cellular networks. The goal of such a procurement review is twofold: (1) ensure 5G, as it involves into critical digital infrastructure, is not vulnerable to opportunistic attacks such as have plagued Internet routing protocols and (2) prevent, to the greatest extent possible, intentional disruption or of communications transmitted across 5G by an adversary nation state.[71] Implementing such a two-prong review in the United States is possible using existing authorities (President's Executive Order on Securing the Information and Communications Technology and Services Supply Chain) and established analytical frameworks (NIST Cybersecurity Framework for technical review and CFIUS or FOCI analysis to assess risk of manipulation or coercion by a nation-state adversary).

Officials conducting this two-prong review would need to adapt the NIST framework to the technical realities of 5G. They would use industry best practices as the standard of review and determine if a particular piece of equipment avoided known risks and included sufficient security protocols to secure the equipment against opportunistic exploit. The controls identified in the NIST framework would serve as a guide for ensuring the review was comprehensive and complete.

For the nation-state adversary analysis, the potential for an adversary's exploitation of vendors' access to networks and the potential for an adversary to manipulate vendor gear to create backdoors are the primary threats. The analysis, however, takes in more than technical risk and focuses an analysis of the vendor's relationship with potential adversaries. Officials must look at the same sorts of risks examined in a CFIUS or Foreign Ownership, Control or Influence (FOCI) review:

a. Record of economic and government espionage against U.S. targets,

b. Record of enforcement and/or engagement in unauthorized technology transfer,

---

https://www.ericsson.com/en/security/a-guide-to-5g-network-security

71. Simone Ferlin, "BGP Internet Routing: What are the Threats?," *Security Intelligence*, December 21, 2017, available at: https://securityintelligence.com/bgp-internet-routing-what-are-the-threats/;

Dev Kundaliya, "BGP Route leak sends European mobile traffic via China," *Computing*, June 10, 2019, available at: https://www.computing.co.uk/ctg/news/3077075/bgp-route-leak-china-telecom

c. The type and sensitivity of the information that shall be accessed,

d. The source, nature and extent of FOCI,

e. Record of compliance with pertinent U.S. laws, regulations and contracts,

f. The nature of any bilateral and multilateral security and information exchange agreements that may pertain, and

g. Ownership or control, in whole or in part, by a foreign government.[72]

IMPLEMENTING A TWO-PRONG SECURITY REVIEW OF FOREIGN-MADE 5G EQUIPMENT IN THE U.S.

The Trump Administration's Executive Order on Communications Technology provides the authority for both elements of this two-prong review of foreign-made equipment destined for future U.S. 5G infrastructure. The work can be carried out by the same agencies that conduct CFIUS reviews under the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA).[73] The President's executive order authorizes not only one-off bans such as Commerce instituted against Huawei, but contains broad language that can be used to justify a systematic review of all foreign-made equipment destined for U.S. 5G networks:

> *The following actions are prohibited: any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service (transaction) by any [US] person . . . where the Secretary of Commerce . . . has determined that:*
>
> *(i) the transaction involves information and communications technology or services designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and*
>
> *(ii) the transaction:*
>
> *(A) poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation,*

72. Defense Counterintelligence and Security Agency, "Foreign Ownership, Control or Influence," DCSA, as of August 11, 2019, available at: https://www.dss.mil/ma/ctp/isia/bams/foci/

73. The lead agent for the 5G two-prong review should be the Secretary of Commerce because his Department contains the National Telecommunications and Information Administration and the National Institute for Standards and Technology, which have the technical acumen to play lead roles in the many technical tasks inherent in this undertaking. In addition, the President's Executive Order on Communications Technology appoints the Department of Commerce as the lead in the inter-agency review process for sanctioning a company.

or maintenance of information and communications technology or services in the United States;

(B) poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States; or

(C) otherwise poses an unacceptable risk to the national security of the United States ….[74]

This language empowers the Secretary of Commerce (in consultation with Treasury, State, DoD, DoJ, and DHS) to determine if any foreign-made equipment purchased by a U.S. entity constitutes a national security risk. Simply put, the comprehensive two-prong 5G risk evaluation that we propose could be instituted as the means by which the Secretary makes this determination.

74. President Donald J. Trump, "Executive Order on Securing the Information and Communications Technology and Services Supply Chain," White House, May 15, 2019, available at: https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/