CONGRESSIONAL TESTIMONY: FOUNDATION FOR DEFENSE OF DEMOCRACIES

House Committee on Energy and Commerce
Subcommittee on Communications and Technology

Securing Communications Networks from Foreign Adversaries

CRAIG SINGLETON

China Program Senior Director and Senior Fellow
Foundation for Defense of Democracies

Washington, DC
February 15, 2024

FDD
FOUNDATION FOR
DEFENSE OF DEMOCRACIES

www.fdd.org

Testimony Summary:

- For years, China has engaged in a concerted effort to exert influence and control over global communications infrastructure. This endeavor extends far beyond technological competition; it strikes at the heart of our national security by threatening the integrity of U.S. and allied information systems.

- China's penetration of U.S. communication networks provides Beijing with direct gateways to intercept and manipulate vast quantities of data traversing our networks, jeopardizing not only the privacy of American citizens but also the integrity of critical infrastructure systems. As a result, China stands poised to impede the mobilization of American military forces, foment a state of disarray, and redirect national attention and resources in both war and short-of-war scenarios.

- China is strategically maneuvering to influence emerging communications technologies and standards, with a clear intent to safeguard its sectoral advantage. The involvement of Chinese companies in international non-profit technology consortia — such as the Linux Foundation and O-RAN Alliance — provide Chinese entities and, by extension, China's party-state the means to influence and possibly control key aspects of next-generation global telecommunications standards and supply chains.

- The recently exposed "Volt Typhoon" operation telegraphs that if tensions with China one day escalate to open conflict, the United States would likely already be at a disadvantage, dealing with compromised command, control, and communication systems that are integral to civilian and military operability. "Volt Typhoon" reflects China's operationalization of a strategy that views peacetime penetration of U.S. networks as a preparatory step for wartime operations — one in which the line between peace and conflict becomes increasingly blurred.

- Operations like "Volt Typhoon" are broadly consistent with People's Liberation Army (PLA) doctrine prioritizing the pre-emptive targeting, penetration, and compromise of "the enemy's information detection sources, information channels, and information-processing and decision-making systems." The stated goal of the PLA's exploitation of adversary infrastructure systems is to "sap the enemy's morale, disintegrate their will to fight, ignite the anti-war sentiment among citizens at home, heighten international and domestic conflict, and weaken and sway the will to fight among its high-level decision makers."

- In the wake of "Volt Typhoon," it is imperative to reassess the resilience of American networks and the strategic imperatives that govern our cyber and national defense policies. The ever-evolving threat posed by China demands the development of policy tools that go beyond the limited prosecutorial reach of the Department of Justice, with the goal of deterring further aggression and compelling Beijing to recalibrate its approach to cyber engagement.

Introduction

Chairman Latta, Ranking Member Matsui, and distinguished members of the subcommittee, I appreciate the opportunity to address you today about a matter of paramount importance to our nation's security — the infiltration of American communications networks by Chinese entities and its implications for our sovereignty and defense.

For years, China has engaged in a concerted effort to exert influence and control over global communications infrastructure. This endeavor extends far beyond technological competition; it strikes at the heart of our national security by threatening the integrity of our information systems. The potential for disruption of communication flows, manipulation of data, and the incapacitation of critical defense and civilian networks jeopardize the foundational pillars of our nation's safety, economic stability, and effective governance.

Section I — China's Communications Sector: A Strategic Challenge to U.S. National Security

Foreign ownership or operation of communication companies does not, in itself, pose an inherent national security risk. However, China stands as a unique case due to its authoritarian governance structure, which extends the Chinese Communist Party's control beyond state-owned enterprises to encompass all private entities. This distinctive dynamic presents a significant challenge to U.S. policymakers, reflecting the fundamental clash of values between Chinese autocracy and liberal democracy. To fully grasp the strategic implications of China's telecommunications industry, one must look beyond China's economic motives and explore how

Chinese policymakers view this sector as a tool to advance China's broader geopolitical ambitions.

China's centrality in the communications sector is not incidental but rather the result of a deliberate strategy outlined in numerous speeches and directives by Chinese leader Xi Jinping, including China's 14th (and most recent) Five-Year Plan. Here, China's communications sector is heralded as "strategic" and "pivotal" in not only advancing China's "next phase of development," but in "establishing new advantages in national competition," presumably over the United States.[1] This framing is broadly consistent with Xi's other stated goal of transforming China into a "cyber superpower" (网络强国建设).[2]

Central to China's ascendancy in the communications realm are its state-owned giants — China Mobile, China Telecom, and China Unicom. These entities, collectively known as the "Big Three," not only dominate China's domestic market but are actively propelled to expand globally.[3] Their expansion serves as a conduit for espionage and subversion, namely because they are subject to exploitation, influence, and control by the Chinese government. For this reason, all three companies have been banned from operating in the United States.

[1] "Translation: 14th Five-Year Plan for National Informatization (December 2021)," *DigiChina*, accessed February 13, 2024. (https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021)

[2] "Translation: Xi Jinping's April 20 Speech at the National Cybersecurity and Informatization Work Conference," *New America*, accessed February 11, 2024. (https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference)

[3] Todd Shields, "FCC Considers Barring China Telecom from U.S. Over Security," *Bloomberg*, December 10, 2020, (https://www.bloomberg.com/news/articles/2020-12-10/fcc-considers-barring-china-telecom-from-u-s-over-security); "China Unicom to Stop U.S. Services," *Federal Communications Commission*, accessed February 13, 2024. (https://www.fcc.gov/consumers/guides/china-unicom-stop-us-services); "FCC Denies China Mobile Telecom Services Application," *Federal Communications Commission*, December 12, 2019. (https://www.fcc.gov/document/fcc-denies-china-mobile-telecom-services-application); "US federal court upholds decision to ban China Telecom," *Datacenter Dynamics*, accessed February 13, 2024 (https://www.datacenterdynamics.com/en/news/us-federal-court-upholds-decision-to-ban-china-telecom/#:~:text=A%20federal%20appeals%20court%20rejected,was%20implemented%20in%20January%202022)

Yet the dual-purpose nature of China's broader communications sector now extends well beyond the "Big Three," encompassing hundreds of other companies, many of which have either evaded U.S. scrutiny or, in some cases, have already established themselves as dominant market players in U.S. and allied markets. This strategic penetration is by design, reflecting China's deliberate efforts to gain leverage over U.S. decision-making and constrain American actions through the strategic control of vital American communication networks.

The heightened threats posed by the Big Three and other Chinese communication companies are rooted in substantial shifts in China's legal and regulatory landscape, effectively subjecting all Chinese enterprises and their employees to the dictates of China's party-state. This legal overhaul, as articulated in China's National Intelligence Law of 2017, mandates unequivocal allegiance, with "all organizations and citizens" compelled to collaborate with state intelligence efforts and maintain secrecy regarding national intelligence operations.[4] Similarly, under China's Cybersecurity Law of 2016, "network operators" are obligated to furnish technical support to public security organs, creating an environment where data traversing global networks supported by Chinese technology is perpetually vulnerable to state intervention, manipulation, or even malicious disruption.[5]

Meanwhile, China is also strategically maneuvering to influence emerging communications technologies and standards, with a clear intent to safeguard its sectoral advantages. Although

[4] "Translation: National Intelligence Law of the People's Republic of China, Art. 7 (adopted 27 June 2017)," *Brown University*, accessed February 12, 2024. (http://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf)

[5] "Translation: Cybersecurity Law of the People's Republic of China, Article. 28 (effective 1 June 2017)," *New America*, accessed February 12, 2024. (https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-lawpeoples-republic-china); Other relevant Chinese laws obligating citizens and organizations to assist in "national security" efforts include the laws on Counterespionage (2014; updated 2023), Counterterrorism (2015), and Cybersecurity (2016).

Open Radio Access Networks (ORAN) promise to reduce costs, increase efficiency, and ensure faster development of new communications technologies — thereby reducing reliance on single vendors, like Huawei — its operationalization is fraught with risks. More specifically, the involvement of Chinese companies in international non-profit technology consortia — such as the Linux Foundation, Open Compute Alliance, RISC-V, and the O-RAN Alliance — provides these companies and, by extension, China's party-state the means to influence and possibly control key aspects of next-generation global telecommunications standards and supply chains.[6]

Notably, The Linux Foundation, pivotal in promulgating open-source software, counts among its top-tier members companies like Huawei, Tencent, Baidu, and WeBank.[7] These entities maintain extensive ties to China's party-state and, in Huawei's case, to China's military. Further intensifying concerns is the composition of the O-RAN Alliance, with a significant portion of its members headquartered in China. Of these, a substantial number have direct ties to the Chinese party-state. At least two-thirds of these companies display elements of Chinese state ownership, and at least 16 O-RAN alliance members maintain public linkages to China's security apparatus.[8] Such links raise more than questions of influence; they also pose infiltration concerns, especially given that all three of China's major mobile operators — China Mobile, China Telecom, and China Unicom — are participants in the O-RAN Alliance.

[6] Rick Switzer, "Open Source Hardware and New Vectors of National Cybersecurity Risk," *Special Competitive Studies Project*, accessed February 13, 2024. (https://www.scsp.ai/wp-content/uploads/2023/01/Open-Source-Hardware-and-New-Vectors-of-National-Cybersecurity-Risk.docx-1.pdf)

[7] "Linux Foundation," *Linux Foundation*, accessed February 12, 2024. (https://www.linuxfoundation.org)

[8] "Membership," *O-RAN Alliance*, accessed February 13, 2024. (https://www.o-ran.org/membership);
Jan-Peter Kleinhans and Tim Rühlig, "The False Promise of Open RAN," *Digital Power China*, accessed February 13, 2024. (https://timruhlig.eu/ctf/assets/x93kiko5rt7l/2VmWvuXxKdqdTuwkLSWUSQ/b48a2ffe9e42dc3a3b09d4c35b1c802e/DPC-Open_RAN_-_FULL_REPORT_-_FINAL.pdf)

Additionally, China's proactive engagement within other international and multilateral organizations, such as the United Nations' International Telecommunications Union (ITU), reflects its determination to shape global telecommunications standards to its advantage. China has aggressively sought to influence the ITU process by, among other things, subsidizing the participation of Chinese non-governmental participation in ITU deliberations and study groups.[9] By steering these international standards, China is positioning itself to set global telecommunication norms that could favor its technologies and strategic interests, potentially embedding dependencies that could be exploited for intelligence gathering or to assert geopolitical leverage.

Despite these and other identified risks, China's cyber activities and broader geopolitical positioning have largely gone unchecked by Washington and its allies, contributing to a concerning climate of impunity. The unintended consequence of today's inaction is that China may one day in the not-so-distant future feel emboldened to launch cyber assaults with the explicit goal of inducing "societal panic," according to Cybersecurity and Infrastructure Security Agency Director Jen Easterly.[10] More specifically, these countervalue operations, including those directed at U.S. civilians, could seek to disrupt essential systems, such as the power grid, financial institutions, healthcare facilities, emergency services, telecommunications networks, and transportation systems.[11]

[9] Brett Schaefer and Danielle Pletka, "Countering China's Growing Influence: The International Telecommunication Union," *The Heritage Foundation*, accessed February 13, 2024. (https://www.heritage.org/global-politics/report/countering-chinas-growing-influence-the-international-telecommunication)

[10] Lawrence Richard, "Chinese Cyberattacks Intended to Induce Societal Panic Across America, Security Directors Tell Congress," *Fox News*, accessed February 13, 2024. (https://www.foxnews.com/politics/chinese-cyber-attacks-intended-induce-societal-panic-across-america-security-directors-tell-congress)

[11] The goal of countervalue targeting is to threaten an adversary with the destruction of its socioeconomic base in order to keep it from initiating a surprise first attack.

Section II — China's Strategic Use of Communication Networks in Modern Warfare

Chinese military discourse has evolved considerably to blur the lines between traditional war and peacetime competition, where the battlefield has no bounds.[12] More specifically, People's Liberation Army (PLA) planners have espoused that "warfare can be military, or it can be quasi-military, or it can be non-military. It can use violence, or it can be nonviolent."[13] This flexible framing aligns with other Chinese military literature that telegraphs the PLA's plans to target foreign communication networks and other soft targets as a means to exert power beyond China's immediate periphery.

To that end, the PLA's extensive corpus on "informaticized" (or cyber) warfare emphasizes achieving information superiority, noting that communication network attacks are the most effective means for a "weak military," like China's, to fight "strong ones," like those of the United States.[14] Such efforts, according to PLA strategists, "should sap the enemy's morale, disintegrate their will to fight, ignite the anti-war sentiment among citizens at home, heighten international and domestic conflict, and weaken and sway the will to fight among its high-level decision makers."[15]

This strategic orientation extends the definition of conflict beyond kinetic engagement to one more consistent with China's broader grand strategy, which leverages non-kinetic means as the

[12] James C. Mulvenon, "Chinese Information Operations Strategies in a Taiwan Contingency," *Testimony Before the U.S.-China Economic and Security Review Commission*, September 15, 2005. (https://www.uscc.gov/sites/default/files/9.15.05mulvenon.pdf)

[13] Qiao Liang and Wang Xiansui (Foreign Broadcast Information Service translation), *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, February 1999).

[14] James C. Mulvenon, "Chinese Information Operations Strategies in a Taiwan Contingency," *Testimony Before the U.S.-China Economic and Security Review Commission*, September 15, 2005. (https://www.uscc.gov/sites/default/files/9.15.05mulvenon.pdf)

[15] James Mulvenon, "China's Revolution in Doctrinal Affairs: Emerging Trends in the Operational Art of the Chinese People's Liberation Army," *Center for Naval Analysis*, January 1, 2002), pp. 271-274.

primary instruments of China's national power. At its core, the PLA's evolving approach to information warfare and cyber operations emphasizes the preemption and exploitation of vulnerabilities in an adversary's information and communication systems. "Seizing the war initiative" (夺取战争主动权), a term PLA war-planners emphasize in operational doctrine, thus centers around pre-emptively targeting, penetrating, and compromising "the enemy's information detection sources, information channels, and information-processing and decision-making systems" through any means necessary.[16]

More specifically, the PLA prioritizes exploiting systemic weaknesses in adversaries' infrastructure systems — what the PLA refers to as "vital points" — rather than adversaries' most fortified systems, including closed, classified systems utilized by the U.S. military. PLA strategists underscore the significance of these "vital points," stating that "disrupt[ing] and damag[ing] the networks of infrastructure facilities … is pivotal to gaining a strategic advantage."[17] This explains, in part, recent observed trends in Chinese state-sponsored cyber operations against U.S. communications infrastructure, including a focus on exploiting public vulnerabilities in major applications — such as Pulse Secure, Apache, F5 Big-IP, and Microsoft products.[18] This, in turn, has facilitated efforts by Chinese cyber actors to penetrate "vital" U.S. sectors, including managed service providers, semiconductor companies, the defense industrial base, universities, and medical institutions.

[16] Alison A. Kaufman and Daniel M. Hartnett, "Managing Conflict: Examining Recent PLA Writings on Escalation Control," *Center for Naval Analysis*, February 2016, accessed February 12, 2024. (https://apps.dtic.mil/sti/pdfs/AD1005033.pdf); Larry M. Wortzel, "The Chinese People's Liberation Army and Information Warfare," *U.S. Army War College*, March 2014, accessed February 13, 2024. (https://apps.dtic.mil/sti/pdfs/ADA596797.pdf)

[17] "Countering Enemy Informationized Operations in Peace and War," *Center for Strategic and Budgetary Assessments*, accessed February 12, 2024. (https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Litigation_Release/Litigation%20Release%20-%20Countering%20Enemy%20Informationized%20Operations%20in%20Peace%20and%20War.pdf); Larry M. Wortzel, "The Chinese People's Liberation Army and Information Warfare," *U.S. Army War College*, March 2014, accessed February 12, 2024. (https://apps.dtic.mil/sti/pdfs/ADA596797.pdf)

[18] "Chinese State-Sponsored Cyber Operations: Observed TTPs," *Cybersecurity and Infrastructure Security Agency*, accessed February 12, 2024. (https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-200b)

The objective, then, in targeting these sectors, according to PLA planners, is to induce a state of "blindness, deafness, and even paralysis" in the opponent, effectively impeding them by severing the flow of critical information and crippling their command-and-control capabilities.[19] To achieve this end, the PLA routinely leverages civilian technological advancements, compelling Chinese companies to serve as force multipliers to assist in these strategic endeavors. This approach aims to combine electronic and computer warfare capabilities into a unified offensive against China's adversaries — which include Washington and Taiwan's government — to incapacitate their information and communication systems while safeguarding China's own.

This strategy, PLA doctrine asserts, is not limited to combat readiness but also includes ensuring China's interests are protected through non-military means, thereby rendering the consequences of military engagement against China prohibitively onerous for its enemies. In other words, the PLA views communication network attacks as a means of deterring or delaying U.S. intervention and compelling adversaries to capitulate before a first shot has ever been fired. It is on this front that China's concept of military-civil fusion becomes increasingly salient. More specifically, PLA planners have emphasized the importance of zeroing in on the "hubs and other crucial links in the systems that move enemy troops, as well their war-making machines, such as harbors, airports, means of transportation, battlefield installations, and the communications, command and control and information systems," many of which rely on hardware and software systems

[19] Larry M. Wortzel, "The Chinese People's Liberation Army and Information Warfare," *U.S. Army War College*, March 2014, accessed February 12, 2024. (https://apps.dtic.mil/sti/pdfs/ADA596797.pdf)

developed and maintained by Chinese companies under legal obligation to assist China's government.[20]

In this milieu of strategic ambiguity, the distinction between Chinese state actors and private entities becomes obscured, reinforcing the doctrine of military-civil fusion. What is more, the PLA encourages Chinese companies to develop capabilities that can be harnessed for military purposes, often through lucrative contracts or favorable access agreements with the government. Such integration underscores the PLA's objective to use every tool at its disposal, including those developed within the civilian sector, to enhance China's position in the international arena and to secure its interests against more technologically advanced adversaries, like the United States.

Section III — China's Cyber Operations: Bridging Theory and Practice

Today's stark reality underscores the significant leverage China holds over the United States, particularly in the realm of technological interdependence. China's penetration of U.S. communication networks provides Beijing with direct gateways to intercept and manipulate vast quantities of data traversing our networks, jeopardizing not only the privacy of American citizens but also the integrity of critical infrastructure systems. As a result, China stands poised to impede the mobilization of American military forces, foment a state of disarray, and redirect national attention and resources in both wartime and short-of-war scenarios. This threat extends to

[20] James C. Mulvenon, "Chinese Information Operations Strategies in a Taiwan Contingency," *Testimony Before the U.S.-China Economic and Security Review Commission*, September 15, 2005. (https://www.uscc.gov/sites/default/files/9.15.05mulvenon.pdf)

potentially disrupting U.S. nuclear communications, according to the Federal Bureau of Investigations.[21]

The recently exposed "Volt Typhoon" operation demonstrates China's strategic pivot from theory to action. [22] This Chinese state-supported cyber initiative compromised thousands of internet-connected devices in an attempt to infiltrate Western critical infrastructure, including naval ports, internet service providers, communications services, and utilities. This bold operation offers a revealing glimpse into China's strategic calculus — showcasing Beijing's willingness to embrace high-risk, short-of-war operations to compromise critical U.S. communication infrastructure, even amidst a so-called diplomatic thaw between the United States and China. Concern surrounding "Volt Typhoon" is amplified by the U.S. Defense Department's 2023 Cyber Strategy, which warns that malicious Chinese activity on U.S. communications systems "informs the PRC's preparations for war."[23] This statement, and others by U.S. national security leaders, underscores the gravity with which Washington views China's cyber operations — not as isolated incidents but as integral components of its military posture.

All told, "Volt Typhoon" embodies the PLA's doctrine of *xianfa zhiren* (先发制人), or "gaining mastery by striking first."[24] It was specifically aimed at penetrating multiple critical infrastructure sectors so that China could cripple key U.S. resources and responses during a

[21] Katie Bo Lillis, "FBI investigating fake communications from US defense systems, including nuclear codes," *CNN*, July 23, 2022, accessed February 13, 2024. (https://www.cnn.com/2022/07/23/politics/fbi-investigation-huawei-china-defense-department-communications-nuclear/index.html)

[22] "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," Cybersecurity & Infrastructure Security Agency (CISA), accessed February 13, 2024. (https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a)

[23] "Summary of the 2023 Department of Defense Cyber Strategy," *U.S. Department of Defense*, accessed February 13, 2024. (https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF)

[24] James C. Mulvenon, Murray Scot Tanner, Michael S. Chase, David Frelinger, David C. Gompert, Martin C. Libicki, and Kevin L. Pollpeter. "Chinese Responses to U.S. Military Transformation and Implications for the Department of Defense." *RAND Corporation*, accessed February 12, 2024. (https://www.rand.org/content/dam/rand/pubs/monographs/2006/RAND_MG340.pdf)

crisis. Moreover, the compromise of SOHO routers with “KV Botnet” malware showcases China’s capability and intent to disguise its digital fingerprints, allowing for a stealthy build-up of offensive cyber capabilities within America’s digital borders.[25]

All told, Volt Typhoon’s implications are profound. By leveraging the interconnectedness of modern infrastructure, China has telegraphed that if tensions one day escalate to open conflict, the United States would already be at a disadvantage, dealing with compromised command, control, and communication systems that are integral to civilian and military operability. Put differently, China’s moves signify a shift to a war footing in cyberspace, where preemptive dominance is the objective. They also reflect China’s operationalization of a strategy that views the peacetime penetration of U.S. networks as a preparatory step for wartime operations — one in which the line between peace and conflict becomes increasingly blurred.

Section V — Policy Recommendations

Operations like “Volt Typhoon” confirm that China has progressed from conceptual models of PLA cyber warfare to active engagement and readiness. This evolution is a clear signal of China’s intent and its determination to integrate cyber operations within its broader strategic objectives. As the United States confronts this stark reality, it becomes imperative to reassess the resilience of American networks and the strategic imperatives that govern its cyber and national defense policies. This ever-evolving threat also demands the development of comprehensive

[25] “U.S. Government Disrupts Botnet of the People’s Republic of China Used to Conceal Hacking of Critical Infrastructure," *U.S. Department of Justice*, accessed February 12, 2024. (https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical)

punitive measures that extend beyond the limited prosecutorial reach of the Department of Justice. Such policy tools must be robust enough to impose significant costs on Chinese entities and individuals involved in perpetrating these crimes, with the goal of deterring further aggression and compelling Beijing to recalibrate its approach to cyber engagement.

Thus far, the U.S. government's policy of incrementally eroding the presence of Chinese technology firms within U.S. networks has provided a partial, albeit imperfect, safeguard against the risks of sabotage within domestic communications infrastructure. This approach also does not specifically address the longer-term challenge of developing trusted global communications networks for use by the United States and its allies. Paradoxically, even as efforts intensify to remove Huawei, ZTE, and DJI equipment from U.S. networks to achieve this goal, Chinese companies appear poised to exploit open-source community collaborations — with the Linux Foundation, O-RAN Alliance, and others — to reintroduce many of today's vulnerabilities into tomorrow's ostensibly trusted networks.

Here, Congress has an important role to play. The White House's engagement with the Linux Foundation, especially in initiatives to bolster cybersecurity through artificial intelligence, underscores the need for a thorough congressional review of these relationships.[26] Other U.S. executive branch agencies have similarly encouraged the use of open standards under development by the O-RAN Alliance. Only through a deeper understanding of these and other

[26] The White House, "Biden-Harris Administration Launches Artificial Intelligence Cyber Challenge to Protect America's Critical Software," August 9, 2023. (https://www.whitehouse.gov/briefing-room/statements-releases/2023/08/09/biden-harris-administration-launches-artificial-intelligence-cyber-challenge-to-protect-americas-critical-software). "Takeaways from the White House Cyber Workforce and Education Summit," *Linux Foundation*, accessed February 13, 2024. (https://www.linuxfoundation.org/blog/blog/takeaways-from-the-white-house-cyber-workforce-and-education-summit); Steven Vaughan-Nichols, "White House joins OpenSSF and the Linux Foundation in securing open-source software," *ZDNet*, accessed February 12, 2024. (https://www.zdnet.com/article/white-house-joins-openssf-and-the-linux-foundation-in-securing-open-source-software)

collaborations can effective legislative measures be crafted to counteract the risk of Chinese infiltration into U.S. and global next-generation communication networks.

Acknowledging the depth of Chinese penetration and influence, it becomes imperative for U.S. legislative and policy responses to evolve, too. Other policy recommendations include:

- Passing legislation that requires the executive branch to concretely identify and evaluate the most likely and consequential Chinese-initiated sabotage scenarios against U.S. and allied communications networks. Such legislation should mandate the development and enforcement of stringent controls to protect against identified threats. Mandatory collaboration with private industry to conduct comprehensive wargaming and network testing should also be prioritized to gauge the potential impacts of Chinese technological tampering on U.S. operational effectiveness, spanning both wartime and peacetime contingencies;

- Amending the Removing Our Unsecure Technologies to Ensure Reliability and Security (ROUTERS) Act to include provisions ensuring collaboration between the Assistant Secretary of Commerce and the Office of the Director of National Intelligence (ODNI) as well as other relevant departments, such as the State Department’s Cybersecurity and Digital Policy Bureau, to enhance oversight and assessment of national security concerns;

- Tying support for the 6G task force with a requirement for a study to ascertain the extent that open-source software, such as that supplied by the Linux Foundation, which is being heavily utilized in the creation of 6G technologies, is either being written or influenced by entities originating from countries of concern;

- Prioritizing subcommittee investigations involving other problematic Chinese communications companies. This includes Tiandy Technologies, which produces genocide-enabling facial recognition software. This company was added to the U.S. Department of Commerce's Bureau of Industry and Security's entity list in 2022 for its role in enabling human rights abuses against Uighur Muslims and its links to Iran's Islamic Revolutionary Guard Corps. Yet, its products remain available for purchase in the United States, and the company has not yet been added to the Federal Communications Commission's Covered List; and

- Launching rigorous oversight and potential restrictions on Chinese battery company CATL's collaborations with U.S. companies, particularly in sectors critical to national security like the communications industry.[27] Such moves should seek to implement robust regulatory frameworks and vigilant monitoring to evaluate technology transfers, investments, and adherence to international standards while assessing the risks associated with CATL's operations given the company's ties to China's government.

[27] Craig Singleton, "Beijing"s Power Play," *Foundation for Defense of Democracies*, accessed October 23, 2023. (https://www.fdd.org/analysis/2023/10/23/beijings-power-play)