**Statement for the Record**
**of**
**Jamil N. Jaffer[1]**
**On**
**Signal Under Siege: Defending America's Communications Networks[2]**
**before the**
**Subcommittee on Telecommunications & Media**
**of the**
**United States Senate Committee on Commerce**

**December 2, 2025**

## I. Introduction

Chairman Fischer, Ranking Member Luján, and Members of the Subcommittee: thank you for inviting me here today to discuss the threats facing America's communication networks and how we might best defend this critical part of our nation's infrastructure.

This hearing comes at a particularly important time in our nation's history, as we see a series of major technological revolutions underway, with artificial intelligence capabilities being brought to bear across a broad range of industries and within our government and that our allies as well, the near-dawn of the quantum computing era, the potential availability of photonics for computing, and expanding access to extremely fast and reliable communications capabilities that permit the transmission of increasingly massive amounts of data around the globe at the speed of light.

At the same time, we also see the very core infrastructure that these new and novel capabilities depend upon being held at risk, under significant threat, by our adversaries, in particular, by nations like China, Russia, Iran, and North Korea and their proxies. The threats posed by these nation-states and those that they support and allow to operate, include efforts to steal our technology at

[1] Jamil N. Jaffer currently serves as Founder & Executive Director of the National Security Institute and the NSI Cyber & Tech Center and as an Assistant Professor of Law and Director of the National Security Law & Policy Program and the Cyber, Intelligence, and National Security LL.M. Program at the Antonin Scalia Law School at George Mason University. Mr. Jaffer is also a Venture Partner at Paladin Capital Group, a leading global multi-stage investor that identifies, supports and invests in innovative companies that develop promising, early-stage technologies to address the critical cyber and advanced technological needs of both commercial and government customers. Mr. Jaffer serves on a variety of public and private boards of directors and advisory boards, including as a member of the Virginia Governor's Task Force on Artificial Intelligence. Among other things, Mr. Jaffer previously served as Chief Counsel & Senior Advisor to the Senate Foreign Relations Committee, Senior Counsel to the House Intelligence Committee, Associate Counsel to President George W. Bush in the White House, and Counsel to the Assistant Attorney General for National Security in the U.S. Department of Justice, as well as a member of the Cyber Safety Review Board at the Department of Homeland Security. Mr. Jaffer is testifying before this Subcommittee in his personal and individual capacity and is not testifying on behalf of any organization or entity, including but not limited to any current or former employer or public or private entity.

[2] Significant portions of this testimony have been drawn in whole or in part from prior testimony provided to the House and Senate by Mr. Jaffer, including, in particular, from Mr. Jaffer's testimony provided to the United States House of Representatives Committee on Energy & Commerce's Subcommittee on Communications & Technology in April 2025. Citations to and quotations marks from such testimony have been omitted, including the significant portions of Mr. Jaffer's prior testimony which have been excerpted verbatim herein.

huge scale, to limit our ability to design, manufacture, and deploy the massive computing infrastructure necessary to sustain and grow these revolutionary capabilities, to prevent us from accessing and using data necessary to train and employ the mathematical models and algorithms that undergird AI and other cutting-edge technologies, to threaten our ability to consistently supply the power needed to drive these technologies, and, perhaps most importantly for today's hearing, to hold at risk the very telecommunications network infrastructure and systems that our people, our companies, and our government rely upon to provide access to these capabilities and to transmit the data around the globe.

Indeed, in recent months and years, we've seen the threat landscape created by nation-state actors and their proxies, expand significantly. Just in the last month, we've learned that Chinese nation-state actors utilized Anthropic's Claude Code capabilities and infrastructure earlier this fall to launch semi-autonomous hacks against nearly three dozen global governments and private sector organizations.[3] And long prior this effort, we've learned about other major threats targeting the both America's cyber and telecommunications infrastructure as well as that of our allies, including actual hacks and capabilities being put in place for destructive attacks—particularly but not exclusively, coming from China and its ruling cabal of the Chinese Communist Party (CCP).

Moreover, while credible reports from last year indicate that the Chinese government has successfully penetrated deep into American telecommunications networks, and has also sought to put in place destructive capabilities at the heart of American and allied critical infrastructure—these efforts, known as Salt Typhoon and Volt Typhoon, respectively, are part of a much larger and more troubling story. As it turns out, there is a significant effort afoot in the cyber domain, architected not just by China, but also by Russia, Iran, and North Korea, and a wide range of proxy actors operating on their behalf, to target America's communications infrastructure, and that of our allies and partners as well.

These efforts are aimed not only at collecting information and intelligence on American government officials and our federal policies and priorities, but also at stealing our intellectual property, collecting massive amounts of data and intelligence on our citizens and, perhaps most troubling, putting in place capabilities that can be used to destructive effect when they choose to do so.

These efforts also stretch across significant parts of our nation's critical infrastructure and are aimed—in various forms—at both the government and key industries, including our financial services, energy, telecommunications, and technology sectors, just to name a few.

While today's hearing is focused on threats to America's communications networks (and the technology that rides on top of it) and assessing what we can do to better defend those networks and systems, it is important that we understand these threats—and our response—in the context of two key issues: (1) the larger national security threat and competition from China, including its key economic and technological elements; and (2) the ongoing and increasingly robust collaboration between our adversaries in China, Russia, Iran, and North Korea.

[3] *See* Anthropic, *Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign* (Nov. 2025), *available online at* <https://assets.anthropic.com/m/ec212e6566a0d47/original/Disrupting-the-first-reported-AI-orchestrated-cyber-espionage-campaign.pdf>.

## II. The Threat Environment Facing America and Our Communications Networks

### A. China

Starting with China, the current Director of National Intelligence, in her first-ever Annual Threat Assessment of the Intelligence Community provided earlier this year, has made clear that the People Republic of China (PRC) "presents the most comprehensive and robust military threat to U.S. national security…[with] a joint force that is capable of full-spectrum warfare" and active efforts ongoing that are "aimed at making the PLA a world-class military by 2049."[4] As a result, the DNI expects that China will seek to remain "in a position of advantage in a potential conflict with the United States…[while also]…conducting wide-ranging cyber operations against U.S. targets for both espionage and strategic advantage."[5]

At the same time, the DNI expects that "Beijing will continue to strengthen its conventional military capabilities and strategic forces, intensify competition in space, and sustain its industrial- and technology-intensive economic strategy to compete with U.S. economic power and global leadership."[6] Moreover, as we think about the most likely flashpoint with China—over Taiwan (which CCP leader Xi Jinping has told his military to be prepared to invade in 2027,[7] just over a year from now)—it is worth noting that the DNI is of the view that "[a] conflict between China and Taiwan would disrupt U.S. access to trade and semiconductor technology critical to the global economy…[and] [e]ven without U.S. involvement in such a conflict, there would likely be significant and costly consequences to U.S. and global economic and security interests."[8]

Speaking specifically about threats to American networks writ large, the DNI has stated unambiguously that China "remains the most active and persistent cyber threat to U.S. government, private-sector, and critical infrastructure networks[,]"[9] further noting that that "China has demonstrated the ability to compromise U.S. infrastructure through formidable cyber capabilities that it could employ during a conflict with the United States."[10] Indeed, the DNI's view is that, if China believes "a major conflict with Washington [is] imminent, it could consider aggressive cyber operations against U.S. critical infrastructure and military assets," with the

---

[4] *See* Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Mar. 2025), at 9, *available online at* <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf>.

[5] *Id*. at 10, *available online at* <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf>.

[6] *Id*. at 9.

[7] *See* William J. Burns, *Transcript: Trainor Award Ceremony Honoring CIA Director William J. Burns* (Feb. 9, 2023), available online at <https://isd.georgetown.edu/2023/02/09/watch-trainor-award-ceremony-honoring-cia-director-william-j-burns/> ("[O]ur assessment at CIA is that I wouldn't underestimate President Xi's ambitions with regard to Taiwan….We know, as a matter of intelligence, that he's instructed the People's Liberation Army to be ready by 2027 to conduct a successful invasion.")

[8] *See 2025 Annual Threat Assessment*, *supra* n. 4 at 11.

[9] *Id*. at 11.

[10] *Id*. at 9.

specific aim of "deter[ring] U.S. military action by impeding U.S. decision-making, inducing societal panic, and interfering with the deployment of U.S. forces."[11]

And this is where the Volt Typhoon and Salt Typhoon efforts by China come into play. The DNI has stated that the Volt Typhoon "campaign [by China] to preposition access on critical infrastructure for attacks during crisis or conflict," and the "more recently identified compromise of U.S. telecommunications infrastructure [by China], also referred to as Salt Typhoon, demonstrates the growing breadth and depth of the PRC's capabilities to compromise U.S. infrastructure."[12]

Truth be told, none of this new when it comes to China. Since at least 2019, over half a decade ago, the U.S. Intelligence Community has been flagging that "China presents a persistent cyber espionage threat and a growing attack threat to our core military and critical infrastructure systems," and specifically warning that China "is improving its cyber attack capabilities," and noting specifically that "China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States."[13]

This drumbeat continued into 2021, with the then-new Administration warning that "China presents a prolific and effective cyber-espionage threat, possesses substantial cyber-attack capabilities, and presents a growing influence threat[,]" and specifically noting that China both "can launch cyber attacks that, at a minimum, can cause localized, temporary disruptions to critical infrastructure within the United States[,]" and noting specifically—for the first time—that China's "cyber-espionage operations have <u>included compromising telecommunications firms</u>, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations."[14]

This was followed, in 2022, with continued warnings of China's "almost certain[]" capability "to launch[] cyber attacks that would disrupt critical infrastructure services within the United States, including against oil and gas pipelines and rail systems," and noting once again the threat to telecommunications, software and other target rich environments.[15]

It is also worth noting that these threats in the cyber domain, including to American communications networks—both historic and ongoing—are undergirded by China's efforts to

---

[11] *Id*. at 12.

[12] *Id*. at 11.

[13] *See* Daniel R. Coats, *Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community* (Jan. 29, 2019), at 5, Senate Select Committee on Intelligence, *available online at* <https://www.intelligence.senate.gov/sites/default/files/documents/os-dcoats-012919.pdf>.

[14] *See* Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Apr. 9, 2021), at 8, *available online at* <https://www.intelligence.senate.gov/sites/default/files/documents/2021-04-09%20Final%20ATA%202021%20%20Unclassified%20Report%20-%20rev%202.pdf> (emphasis added).

[15] *See* Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Feb. 7, 2022), at 8, *available online at* <https://intelligence.house.gov/uploadedfiles/hhrg_117_ig00_wstate_hainesa_20220308.pdf>.

"dominat[e] global markets and strategic supply chains…making other nations dependent on China[,]" particularly in areas that are critical to United States technology leadership, such as critical minerals, semiconductors, and artificial intelligence.[16] For example, the current DNI has made clear that "China's dominance in the mining and processing of several critical materials is a particular threat, providing it with the ability to restrict quantities and affect global prices."[17] We also know that China seeks to "become a global [science and technology] superpower, surpass the United States, promote self-reliance, and achieve further economic, political, and military gain...[by] prioritiz[ing] technology sectors such as advanced power and energy, AI, biotechnology, quantum information science, and semiconductors."[18]

And the tie-in between these efforts and the threats to our telecommunications and cyber infrastructure is that the Chinese are actively exploiting our communications networks to juice their efforts to become a technology superpower. They are doing so in a range of ways, including engaging in intellectual property theft at industrial scale, with the DNI noting that China is directly stealing "hundreds of gigabytes of intellectual property from companies in Asia, Europe, and North America in an effort to leapfrog over technological hurdles, with as much as 80 percent of U.S. economic espionage cases as of 2021 involving PRC entities."[19] China also use its intelligence collection capabilities on U.S. networks to identify investments, recruit talent, evade sanctions, and conduct cyber operations, all of which are key parts of their effort to "accelerat[e] [China's] S&T progress through a range of licit and illicit means."[20]

And it is worth noting that China's ongoing "multifaceted, national-level strategy designed to displace the United States as the world's most influential AI power by 2030,"[21] is not simply aimed at economic gain but is also designed to support China's intelligence collection efforts and its larger plan to undermine American national security.

Indeed, the current DNI has made clear that "Chinese AI firms are already world leaders in voice and image recognition, video analytics, and mass surveillance technologies," and that the "[t]he PLA probably plans to use large language models (LLMs) to generate information deception attacks, create fake news, imitate personas, and enable attack networks."[22]

It goes without saying that these Chinese intelligence collection efforts and covert and overt messaging operations take place over the entirety of America's communications networks. One obvious example is very real threat posed by TikTok to America's national security.[23] While many

---

[16] *See 2025 Annual Threat Assessment*, *supra* n. 4 at 12.

[17] *See id*.

[18] *Id*. at 13.

[19] *Id*.

[20] *Id*.

[21] *Id*.

[22] *Id*.

[23] *See, e.g.*, *Protecting Americans from Foreign Adversary Controlled Applications Act*, Pub. L. No. 118-50, div. H, 138 Stat. 955 (2024); The White House, *Protecting Americans' Sensitive Data from Foreign Adversaries*, 86 Fed.

Americans—and perhaps some key leaders and policymakers—view TikTok primarily as a way to watch a bunch of kid and dog videos, the fact is that TikTok's extensive collection of data on Americans and our allies, its ties to the Chinese Communist Party, and the Chinese government's influence over TikTok's algorithm, makes it a unique and serious national security threat. [24]

Indeed, when one combines the massive amount of data that TikTok collects on its users with other data stolen by Chinese government hackers, including security clearance files and the sensitive financial, health, and travel data of millions of Americans, it is clear that the Chinese government can use this data—powered by AI—to drive future sophisticated intelligence collection and disinformation campaigns targeting Americans and our allies.[25]

As if this weren't enough, it is worth noting that China also seeks to increase its already central role in the semiconductor supply chain to undermine U.S. communications networks, including our ability to build them and to secure them. The DNI has identified that the China has "made progress in producing advanced 7-nanometer (nm) semiconductor chips for…cellular devices using previously acquired deep ultraviolet (DUV) lithography equipment," and has noted that while they may face volume production challenges, China is also continuing to "explore applying advanced patterning techniques to DUV machines to produce semiconductor chips as small as 3nm,"[26] a claim that appears to be supported by reporting earlier this year that Chinese semiconductor company SMIC has managed to manufacture 5 nm chips using such techniques with DUV machines.[27] And, of course, the DNI rightly notes that "China [already] leads the world in legacy logic semiconductor (28nm and up) production, accounting for 39.3 percent of global capacity, and is expected to add more capacity than the rest of the world combined through 2028[,]" for chips that are "vital to producing automobiles, consumer electronics, home appliances, factory automation, broadband, and many military and medical systems,"[28] including critical parts of our telecommunications networks and systems.

Indeed, China has long sought to infiltrate U.S., allied, and other global communications networks with their own equipment, both by building it on the cheap using stolen U.S. technology and then innovating on top of it, as well as by heavily subsidizing the sale of such equipment. The stories of how companies like Huawei and ZTE built their core networking capabilities and got them

---

Reg. 31423 (June 9, 2021); The White House, *Addressing the Threat Posed by TikTok*, 85 Fed. Reg. 48637-38 (Aug. 6, 2020).

[24] *See Brief of Amicus Curiae Former National Security Officials*, *TikTok Inc., et al. v. Merrick B. Garland*, No. 24-1113 (S. Ct.) (filed Dec. 27, 2024), *available online at* <https://www.supremecourt.gov/DocketPDF/24/24-656/336098/20241227135716235_24-656%2024-657bsacFormerNationalSecurityOfficials.pdf>.

[25] *Id*. at 4-13.

[26] *See 2025 Annual Threat Assessment*, *supra* n. 4 at 14.

[27] *See* Ananya Gairola, *China's Chip Breakthrough Without ASML Makes Chamath Palihapitiya Take Stock Of Beijing's 'Formidable' Nature: 'America Can Win If…'*, Benzinga (Apr. 23, 2025), *available online at* <https://www.benzinga.com/tech/25/04/44970472/chinas-chip-breakthrough-without-asml-makes-chamath-palihapitiya-take-stock-of-beijings-formidable-nature-america-can-win-if>.

[28] *See 2025 Annual Threat Assessment*, *supra* n. 4 at 13.

deployed globally are well known,[29] and multiple Congressional committees and U.S. administrations have sought to highlight the threat to our own infrastructure and that of our allies,[30] and the relative success of the U.S. domestic rip-and-replace program can serve as a model for other nations as well.[31] But the challenges continue. A recent report from the U.S.-China Economic and Security Review Commission (USCC) notes Chinese critical infrastructure investments in various strategic locations around globe, including in the Middle East, Southeast Asia, and Africa, noting, for example, that China's investment into Southeast Asia's information and communications technology sector exceeds $12 billion and is focused on areas like cloud computing, data center capacity, and core network equipment provision for national telecommunications infrastructure.[32] Taking a page from the U.S. book, the USCC notes that while today Huawei supplies 70 percent of Indonesia's network equipment, it "has offered to take over the remaining percentage with a free rip-and-replace program."[33] This approach is almost certainly being mirrored in strategic locations around the globe.

China has also targeted the undersea cables that serve as the backbone of the international communications system, which carries 95% of global Internet traffic and around 99% of transoceanic digital communications.[34] The USCC report notes that China is "increasingly engaged in undersea cable-cutting activities as a gray zone pressure tactic, and there is mounting evidence that Beijing is developing new cable-cutting technologies for potential wartime use."[35] The USCC goes on to note that "[f]or over a decade, Chinese scientists at research institutions affiliated with the PLA have actively researched strategies for severing undersea cables, acquiring numerous patents for technologies designed to cut deep-sea cables more cheaply and efficiently" and that earlier this year, the China Ship Scientific Research Center (a U.S. sanctioned entity) "unveiled a new design for an 'electric cutting device for deep-sea cables' reportedly capable of severing armored cables at depths of more than 13,000 feet."[36] Indeed, the USCC reports that "Chinese vessels have sabotaged critical undersea cables near Taiwan and in the Baltic Sea" and notes two incidents in 2025 alone, where "Chinese-owned 'shadow fleet' vessels cut cables near Taiwan while engaging in highly irregular movement patterns and disguising their identities and locations as well as a November 2024 incident where a "Chinese vessel severed two undersea cables in the Baltic Sea—one connecting Sweden and Lithuania, the other connecting Germany and Finland—after dragging its anchor for more than 100 miles," which European investigators

---

[29] *See, e.g.*, Jill C. Gallagher, *U.S. Restrictions on Huawei Technologies: National Security, Foreign Policy, and Economic Interests*, Congressional Research Service (Jan. 5, 2022), at 6-12, *available online at* <https://www.congress.gov/crs_external_products/R/PDF/R47012/R47012.2.pdf>.

[30] *Id*. at 12-39.

[31] *Id*. at 22-25.

[32] *See* U.S.-China Economic and Security Review Commission, *2025 Report to Congress* (Nov. 2025), at 233-34, *available online at* <https://www.uscc.gov/sites/default/files/2025-11/2025_Annual_Report_to_Congress.pdf>.

[33] *Id*. at 234.

[34] *See* Jill C. Gallagher, *Undersea Telecommunication Cables: Technology Overview and Issues for Congress*, Congressional Research Service (Sept. 13, 2022), *available online at* <https://www.congress.gov/crs_external_products/R/PDF/R47237/R47237.2.pdf>.

[35] *See USCC 2025 Report*, *supra* n. 32 at 98.

[36] *Id*.

believe was a joint Russia-China operation.[37] And this doesn't even cover the potential tapping threat posed by Chinese cable repair vessels nor the relative lack of allied repair capacity in the IndoPacific (as well as globally) noted by the USCC.[38]

Finally, when it comes to the threats posed by China to American communication networks, we cannot forget about China's efforts to compete with the United States in the space domain and, in particular, its ability to potentially take action against the United States in that arena. While it is true that in recent decades, the long-haul telecommunications infrastructure has pivoted from satellite-based communications to undersea cables as noted above, the reality is that we are increasingly relying on space-based assets for a range of services and capabilities that are critical to our communications capabilities, including position, navigation, and timing, as well as broadband access across the globe, both for government and industry use cases. As such, China's rapidly developing capabilities in intelligence, surveillance, and reconnaissance (ISR), where the DNI finds that it has "achieved global coverage…in some of its…constellations and world-class status in all but a few space technologies[,]" as well as its Beidou constellation which competes with our GPS system, and its recent launch of a low Earth orbit (LEO) constellation for satellite Internet services,[39] are all concerning trends.

These trends, of course, are also particularly concerning when viewed in light of China's counterspace capabilities, which the DNI has made clear "will be integral to PLA military campaigns," particularly given that "China has counterspace-weapons capabilities intended to target U.S. and allied satellites."[40] Chinese capabilities to go after America's space-based communications infrastructure don't just include "ground-based counterspace capabilities, including EW systems, directed energy weapons (DEWs), and antisatellite (ASAT) missiles intended to disrupt, damage, and destroy target satellites," but also includes "orbital technology demonstrations…[and] on-orbit satellite inspections of other satellites," capabilities that "while not counterspace weapons tests, prove [China's] ability to operate future space-based counterspace weapons…[and] which probably would be representative of the tactics required for some counterspace attacks."[41]

For its part, the Federal Communication's Commission under its new chairman has sought to take action to address the threats posed by China and other threat actors. For example, the FCC recently established a Council on National Security aimed at leveraging the FCC's authorities to counter foreign adversaries, like China, with the goals of reducing the American technology and communications sectors' supply chain dependencies on such adversaries; mitigating America's vulnerabilities to cyberattacks, espionage, and surveillance; and ensuring U.S. victory in our strategic competition with China in critical technology domains like AI, space, next gen

[37] *Id*.

[38] *Id*. at 99.

[39] *See 2025 Annual Threat Assessment*, *supra* n. 4 at 15.

[40] *Id*.

[41] *Id*.

communications, and quantum computing.[42] The FCC has also taken action in a range of areas including foreign ownership, control, and influence over FCC licensees,[43] foreign controlled labs,[44] and the security of submarine cables,[45] to name just a few.

### B. Russia

Turning to Russia, it is clear—and the current DNI agrees—that "Russia's current geopolitical, economic, military, and domestic political trends underscore its resilience and enduring potential threat to U.S. power, presence, and global interests[,]" and that Russian President Vladimir Putin is "prepared to pay a very high price to prevail in what he sees as a defining time in Russia's strategic competition with the United States, world history, and his personal legacy."[46] Indeed, the DNI believes that "Moscow's massive investments in its defense sector will render the Russian military a continued threat to U.S. national security," noting that Russia has "increased its defense budget to its heaviest burden level during Putin's more than two decades in power," while also "import[ing] munitions such as UAVs from Iran and artillery shells from North Korea… enhancing the threat its military poses."[47]

Like China, Russia's "disinformation, espionage, influence operations, military intimidation, cyberattacks, and gray zone tools…[are also part of an effort] to try to compete below the level of armed conflict and fashion opportunities to advance Russian interests."[48] Indeed, the current DNI has made clear that Russia's cyber-enabled "influence activities…including [] stoking political discord in the West, sowing doubt in democratic processes and U.S. global leadership, degrading Western support for Ukraine, and amplifying preferred Russian narratives…will continue for the foreseeable future and will almost certainly increase in sophistication and volume."[49] And current DNI's view is that Russian "information operations efforts to influence U.S. elections are advantageous, regardless of whether they affect election outcomes, because reinforcing doubt in the integrity of the U.S. electoral system achieves one of [Russia's] core objectives."[50]

---

[42] *See* Federal Communications Commission, *FCC Council on National Security*, *available online at* <https://www.fcc.gov/fcc-council-national-security>.

[43] *See* Federal Communications Commission, *Protecting our Communications Networks by Promoting Transparency Regarding Foreign Adversary Control*, Notice of Proposed Rulemaking (May 22, 2025), *available online at* <https://docs.fcc.gov/public/attachments/FCC-25-28A1.pdf>.

[44] *See* Federal Communications Commission, *FCC Takes Action on "Bad Labs" Apparently Controlled By China* (Sept. 25, 2025), *available online at* <https://docs.fcc.gov/public/attachments/DOC-414369A1.pdf>.

[45] *See* Federal Communications Commission, *Review of Submarine Cable Landing License Rules and Procedures to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks,* Report and Order and Further Notice of Proposed Rulemaking (Aug. 7, 2025), *available online at* <https://docs.fcc.gov/public/attachments/FCC-25-49A1.pdf>.

[46] *See 2025 Annual Threat Assessment*, *supra* n. 4 at 16.

[47] *Id*. at 18.

[48] *Id*.

[49] *Id*. at 20.

[50] *Id*.

The fact, of course, is that much of these efforts, take place through Russia's cyber exploitation of American communications and technology networks and systems. Specifically, the DNI has determined that "Russia's advanced cyber capabilities, its repeated success compromising sensitive targets for intelligence collection, and its past attempts to pre-position access on U.S. critical infrastructure make it a persistent counterintelligence and cyber attack threat."[51]

Such capabilities should be a major concern for the United States because the "practical experience [Russia] has gained integrating cyber attacks and operations with wartime military action…[will] almost certainly amplify[] its potential to focus combined impact on U.S. targets in [a] time of conflict."[52] Indeed, the DNI assesses that Russia's "demonstrat[ion] [of] real-world disruptive capabilities during the past decade, including gaining experience in attack execution by relentlessly targeting Ukraine's networks with disruptive and destructive malware[,]"[53] provides Moscow with a "unique strength" in the cyber domain.[54]

As with China, however, these facts should not be surprising, particularly given that since at least 2019, the United States has been raising concerns about Russia's efforts to "map[] our critical infrastructure with the long-term goal of being able to cause substantial damage," and given that the then-DNI, Senator Dan Coats, specifically disclosed that Russia was actively "staging cyber attack assets to allow it to disrupt or damage US civilian and military infrastructure during a crisis."[55]

This is the exact same kind of deployment of cyber capabilities that we saw Volt Typhoon put in place more recently on behalf of the Chinese government. Indeed, as one thinks about the capabilities that a nation like Russia has available to target American telecommunications systems and networks today, it is worth noting that back in 2019, the then-DNI stated that "Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure—such as disrupting an electrical distribution network for at least a few hours[.]"[56]

And these concerns only grew more troubling, particularly for our telecommunication's infrastructure, in 2021 and 2022, when the DNI specifically noted that "Russia continues to target critical infrastructure, including underwater cables and industrial control systems, in the United States and in allied and partner countries, as compromising such infrastructure improves—and in some cases can demonstrate—its ability to damage infrastructure during a crisis."[57]

Russia, like China, is also focused on American undersea cables. For at least a decade, news reports have flagged the threat that Russian ships pose to American undersea cable networks

---

[51] *Id*. at 19.

[52] *Id*.

[53] *Id*. at 20.

[54] *Id*. at 19.

[55] *See 2019 Worldwide Threat Assessment*, *supra* n. 13 at 6.

[56] *Id*.

[57] *See 2021 Annual Threat Assessment*, *supra* n. 14 at 9; *2022 Annual Threat Assessment*, *supra* n. 15 at 12.

systems, both from a damage perspective as well as from an intelligence collection capability.[58] And in 2023, the Congressional Research Service noted that as far back in 2018, the Associated Press cited a Russian publication for the proposition that "Russia has the capability to cut cables, connect to top-secret cables, and jam underwater sensors that detect intrusions" raising significant concern for the NATO allies, among others.[59]

Like China, as well, it is worth noting Russia also has advanced "space programs threaten the Homeland, U.S. forces, and key warfighting advantages,"[60] and that "Russia continues to train its military space elements and field new antisatellite weapons to disrupt and degrade U.S. and allied space capabilities[, including by]….expanding its arsenal of jamming systems, DEWs, on-orbit counterspace capabilities, and ASAT missiles designed to target U.S. and allied satellites."[61]

It is also clear that "Russia has proven adaptable and resilient, in part because of the expanded backing of China, Iran, and North Korea[,]"[62] that "Russia's relationship with China has helped Moscow circumvent sanctions and export controls to continue the war effort, maintain a strong market for energy products, and promote a global counterweight to the United States, even if at the cost of greater vulnerability to Chinese influence[,]" and that Russia's "increase[ed] military cooperation with Iran and North Korea… continue[s] to help its war effort[.]"[63]

### C. Iran

Members of this Committee are also well aware of the significant threat that Iran poses to American national security and our interests, allies, and partners globally, including our longstanding allies in the Middle East, including Israel, Jordan, Saudi Arabia, the United Arab Emirates, and Bahrain, to name a few. This threat is perhaps most clear in the Iranian regime's support of all manner of terrorist groups around the world from Hizballah to Hamas and Palestinian Islamic Jihad to the Yemeni Houthis and groups in Iraq and Syria that have directly attacked—and kidnapped and killed—Americans citizens and soldiers for years. The DNI recently made clear

---

[58] *See, e.g.*, David E. Sanger & Eric Schmitt, *Russian Ships Near Data Cables Are Too Close for U.S. Comfort*, New York Times (Oct. 26, 2015), *available online at* <https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html>; *see also, e.g.,* Morgan Chalfant & Olivia Beavers, *Spotlight Falls on Russian Threat to Undersea Cables*, The Hill (June 17, 2018), *available online at* <https://thehill.com/policy/cybersecurity/392577-spotlight-falls-on-russian-threat-to-undersea-cables/>; CBS News, *Concern over Russian Ships Lurking Around Vital Undersea Cables* (Mar. 30, 2018), *available online at* <https://www.cbsnews.com/news/russian-ships-undersea-cables-concern-vladimir-putin-yantar-ship/>; Michael Birnbaum, *Russian Submarines Are Prowling Around Vital Undersea Cables. It's Making NATO Nervous*, Washington Post (Dec. 22, 2017), *available online at* <https://www.washingtonpost.com/world/europe/russian-submarines-are-prowling-around-vital-undersea-cables-its-making-nato-nervous/2017/12/22/d4c1f3da-e5d0-11e7-927a-e72eac1e73b6_story.html>.

[59] *See* Jill C. Campbell, *Protection of Undersea Telecommunication Cables: Issues for Congress*, Congressional Research Service (Aug. 7, 2023), at 7, *available online at* <https://www.congress.gov/crs_external_products/R/PDF/R47648/R47648.4.pdf>.

[60] *See 2025 Annual Threat Assessment*, *supra* n. 4 at 19.

[61] *Id*. at 20.

[62] *Id*. at 16.

[63] *Id*. at 17.

that Iran "will continue to directly threaten U.S. persons globally and remains committed to its decade-long effort to develop surrogate networks inside the United States…[including] seek[ing] to target former and current U.S. officials it believes were involved in the killing of…IRGC[]-Qods Force Commander Qasem Soleimani in January 2020[, having] previously [] tried to conduct lethal operations in the United States."[64]

And we well know of Iran's longstanding efforts to pursue nuclear weapons capabilities, against the interests of the United States and our allies. But it is also worth noting that Iran is also building up—and sharing with other U.S. adversaries—its conventional weapons capabilities as well. Indeed, according to the DNI, "Iranian investment in its military has been a key plank of its efforts to confront diverse threats and try to deter and defend against an attack by the United States or Israel[,]" including through its efforts to "bolster the lethality and precision of its domestically produced missile and UAV systems,"[65] and to share them with countries like Russia, which has long been using Iranian Shaheed drones in Ukraine.

But the one of the most important—and undercounted—threats posed by Iran are its efforts in the cyber domain, including its efforts to target our telecommunications networks and systems. Specifically, according to the DNI, "Iran's growing expertise and willingness to conduct aggressive cyber operations also make it a major threat to the security of U.S. and allied and partner networks and data."[66]

Indeed, the current DNI has noted that "[g]uidance from Iranian leaders has incentivized cyber actors to become more aggressive in developing capabilities to conduct cyber attacks."[67] This is particularly concerning because in 2019, the-DNI Coats told Congress that Iran was "attempting to deploy cyber attack capabilities that would enable attacks against critical infrastructure in the United States and allied countries," and that it was then "capable of causing localized, temporary disruptive effects—such as disrupting a large company's corporate networks for days to weeks—similar to its data deletion attacks against dozens of Saudi governmental and private-sector networks in late 2016 and early 2017."[68]

And we also know that "Iran often amplifies its influence operations with offensive cyber activities[,]" including efforts during the last election cycle to acquire information from the President's campaign and to "manipulate U.S. journalists into leaking [the] information illicitly acquired from the campaign."[69]

These capabilities and efforts demonstrate Iran's interest in and ability to target and use American communications systems to undermine our national security. When combined with the challenges of effectively deterring an actor like Iran, as well as the limited efforts the United States has

---

[64] *Id*. at 22.

[65] *Id*.

[66] *Id*.

[67] *Id*.

[68] *See 2019 Worldwide Threat Assessment*, *supra* n. 13 at 6.

[69] *See 2025 Annual Threat Assessment*, *supra* n. 4 at 26.

historically taken to establish real deterrence in the cyber domain by being relatively unwilling to impose significant consequences, the potential for a strategic miscalculation increases significantly as does the threat to American communications networks.

### D. North Korea

The DNI also assesses that North Korea will "continue to pursue strategic and conventional military capabilities that target the [United States], threaten U.S. and allied armed forces and citizens, and …undermine U.S. power and reshape the regional security environment in [North Korea's] favor."[70]

North Korea's focus, in the cyber domain, is targeting American telecommunications networks and the financial institutions that ride upon them to "fund[] its military development—allowing it to pose greater risks to the United States—and economic initiatives by stealing hundreds of millions of dollars per year in cryptocurrency."[71] However, the DNI also assesses that North Korea "may also expand its ongoing cyber espionage to fill gaps in the regime's weapons programs, potentially targeting defense industrial base companies involved in aerospace, submarine, or hypersonic glide technologies."[72]

Like with China, Russia, and Iran, much of this unsurprising because we knew back in 2019 that "North Korea poses a significant cyber threat to financial institutions [and] remains a cyber espionage threat…us[ing] cyber capabilities to steal from financial institutions to generate revenue[,]…includ[ing] attempts to steal more than $1.1 billion from financial institutions across the world [and]…a successful cyber heist of an estimated $81 million from the New York Federal Reserve account of Bangladesh's central bank."[73]

We also learned, interestingly, in 2019 that North Korea "retains the ability to conduct disruptive cyber attacks,"[74] a capability that we more recently learned was focused on American cyber networks. Specifically, in 2021, the DNI told Congress that that "Pyongyang probably possesses the expertise to cause temporary, limited disruptions of some critical infrastructure networks and disrupt business networks in the United States, judging from its operations during the past decade, and [further that] it may be able to conduct operations that compromise software supply chains."[75] We also learned, in 2022, that "Pyongyang is well positioned to conduct surprise cyber attacks given its stealth and history of bold action."[76]

As with Iran, given North Korea's burgeoning capacity and willingness to conduct operations in the cyber domain, and the relative challenges of using deterrence against a nation like North Korea

---

[70] *Id*.

[71] *Id*. at 28.

[72] *Id*.

[73] *See 2019 Worldwide Threat Assessment*, *supra* n. 13 at 6.

[74] *Id*.

[75] *See 2021 Annual Threat Assessment*, *supra* n. 14 at 14; *2022 Annual Threat Assessment*, *supra* n. 15 at 17.

[76] *See 2022 Annual Threat Assessment*, *supra* n. 15 at 17.

poses, as well as the limited willingness of the United States to engage in more generally deterrence in the cyber domain, the potential for a tactical miscalculation—and the concomitant threat to American communications networks—is more significant than one might initially assume.

## III. Assessing the Threats to America's Communications Infrastructure

When we look across the totality of the threats to America's communications infrastructure posed these four major nation-state threat actors—China, Russia, Iran, and North Korea—what becomes increasingly clear is that it is virtually impossible for any one private sector actor, or even any single industry in the United States alone, writ-large, to effectively combat these the scale, scope and nature of these threats.

We are faced today with a nonstop, day-in, day-out, military-grade assault on our nation's critical infrastructure and that of our allies. This effort is being undertaken by multiple military and intelligence organizations across multiple adversary countries and is focused on the core networks, systems, and technologies that support our governments, telecommunications systems, banking networks, energy grids, and healthcare institutions, just to name a few important ones.

While this assault is not always aimed the destruction or disruption of these networks, systems, or technologies, even the intelligence collection and information operations that our adversaries are running can have massive implications for our economic and national security. They can enable mass-scale intellectual property theft—much of which is already taking place—and thereby undermine America's innovation-driven economy while bootstrapping nations like China. They can also undermine government institutions and cut out basic support for the rule of law across the globe. And they can enable future military and intelligence operations against our nations and its allies. Even more troublingly, we are seeing nation-state adversaries put in place the very capabilities that would enable them to engage in large-scale, sustained disruptions of American and allied critical infrastructure, including key telecommunications networks and systems.

The question then is what is to be done about these threats posed to our core networks, systems, and technologies. As a nation, the stark reality is we are not currently positioned to provide for a comprehensive defense of our nation—nor the very communications systems or networks that American companies help operate—and we do not appear prepared to undertake the actions needed to do so.

One need only look at the Salt Typhoon hacks aimed at our communications infrastructure—primarily for intelligence collection—to understand just how vulnerable (and underprepared) we are to deal with these adversaries. In that case, we learned—after years and years of knowing that the Chinese government and its military and intelligence institutions were focused on this effort—that China had obtained widescale access to our telecommunications networks.[77] Specifically, the

[77] *See* Chris Jaikaran, *Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications*, Congressional Research Service (Jan. 23, 2025), *available online at* <https://www.congress.gov/crs_external_products/IF/PDF/IF12798/IF12798.15.pdf> ("In early October 2024, media outlets reported that People's Republic of China (PRC) state-sponsored hackers infiltrated United States telecommunications companies (including internet service providers)….[P]ublic reporting suggests that the hackers may have targeted the systems used to provide court-approved access to communication systems used for investigations by law enforcement and intelligence agencies. PRC actors may have sought access to these systems

FBI stated that China's "targeting of commercial telecommunications infrastructure has revealed a broad and significant cyber espionage campaign," and that Chinese-affiliated actors "have compromised networks at multiple telecommunications companies to enable the theft of customer call records data, the compromise of private communications of a limited number of individuals who are primarily involved in government or political activity, and the copying of certain information that was subject to U.S. law enforcement requests pursuant to court orders."[78]

This was an astounding event; according to the then-Chairman of the Senate Intelligence Committee, Senator Mark Warner (D-VA), it was the "worst telecom hack in our nation's history — by far,"[79] and according the then-Vice Chair of the Committee (and now current Secretary of State and National Security Advisor) Senator Marco Rubio (R-FL) referred to the hack as "an egregious, outrageous and dangerous breach of our telecommunications systems across multiple companies[.]"[80]

And yet, after the reported convening of a White House Unified Coordination Group (UCG),[81] a lengthy (and apparently still ongoing) law enforcement investigation,[82] and a nascent (and incomplete) investigation by the Cyber Safety Review Board (of which I was once a member),[83] not to mention a rushed regulatory effort by the Federal Communications Commission[84] (which

---

and companies to gain access to presidential candidate communications. With that access, they could potentially retrieve unencrypted communication (e.g., voice calls and text messages).")

[78] *See* Federal Bureau of Investigations, *Joint Statement from FBI and CISA on the People's Republic of China Targeting of Commercial Telecommunications Infrastructure* (Nov. 14, 2024), *available online at* <https://www.fbi.gov/news/press-releases/joint-statement-from-fbi-and-cisa-on-the-peoples-republic-of-china-targeting-of-commercial-telecommunications-infrastructure>.

[79] Ellen Nakashima, *Top Senator Calls Salt Typhoon "Worst Telecom Hack in our Nation's History,"* Washington Post (Nov. 21, 2024), *available online at* <https://www.washingtonpost.com/national-security/2024/11/21/salt-typhoon-china-hack-telecom/>.

[80] Patrick Maguire, *Sen. Marco Rubio Says Chinese Hacking of U.S. Telecom Companies is a "Very Serious Situation that we Face*," CBS News (Nov. 3, 2024), *available online at* <https://www.cbsnews.com/news/marco-rubio-chinese-hacking-american-telecom-companies/>.

[81] *See, e.g.*, Ellen Nakashima, *White House Forms Emergency Team to Deal with China Espionage Hack*, Washington Post (Nov. 11, 2024) ("The White House on Tuesday convened a meeting of deputy secretaries of key agencies to stand up what's known as a 'unified coordination group.' The group's role is to ensure there is consistent interagency visibility into the response by the FBI, the Office of the Director of National Intelligence, and the Department of Homeland Security's Cybersecurity and Information Security Agency (CISA)."); *see also Salt Typhoon Hacks*, *supra* n. 61 at 2 (discussing Salt Typhoon and noting that "[b]y publicly available counts, this is the fourth time that the U.S. government has established a Cyber UCG—which were previously established for China's compromise of Microsoft Exchange services in 2021, Russia's compromise of SolarWinds in 2021.")

[82] *See, e.g.*, Federal Bureau of Investigation, *FBI Seeking Tips about PRC-Targeting of US Telecommunications* (Apr. 24, 2025), *available online at* <https://www.ic3.gov/PSA/2025/PSA250424-2>.

[83] Martin Matishak, *Cyber Incident Board's Salt Typhoon Review to Begin Within Days, CISA Leader Says*, The Record (Dec. 3. 2024), *available online at* <https://therecord.media/salt-typhoon-csrb-review>.

[84] *See* Federal Communications Commission, *Protecting the Nation's Communications Systems from Cybersecurity Threats*, Declaratory Ruling and Notice of Proposed Rulemaking (Jan. 15, 2025), *available online at* <https://docs.fcc.gov/public/attachments/FCC-25-9A1_Rcd.pdf>; *see also* Federal Communications Commission, *Chairwoman Rosenworcel Announces Agency Action to Require Telecom Carriers to Secure their Networks* (Dec. 5, 2024), *available online at* <https://docs.fcc.gov/public/attachments/DOC-408013A1.pdf>.

has since been reversed by the current FCC in favor of a number of more focused actions directed at the Chinese threat as noted above and in line with a more "agile and collaborative approach to cybersecurity that has proven successful"),[85] the release of two security guidance documents jointly released by a significant number of law enforcement and intelligence agencies from multiple allied countries,[86] and legislation introduced,[87] we have precious little substantive action to show for this hack.

According to press reports, at least some of the telecommunications companies involved have managed to remove the attackers (or at least those they could identify),[88] and the breadth of the hack appears to have been global, affecting at least nine telecommunications companies,[89] at least a dozen nations,[90] and targeting senior U.S. government officials,[91] with significant amounts of metadata and the content of certain individuals' communications obtained.[92] And the FCC, while reversing its earlier rush to regulation, has obtained series of commitments from American communications companies to upgrade their cybersecurity practices by taking coordinated actions

---

[85] *See* Federal Communications Commission, *Protecting the Nation's Communications Systems from Cybersecurity Threats*, Order on Reconsideration (Nov. 20, 2025), *available online at* <https://docs.fcc.gov/public/attachments/FCC-25-81A1.pdf>.

[86] *See* National Security Agency, et al., *Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System* (Aug/Sept. 2025), *available online at* <https://media.defense.gov/2025/Aug/22/2003786665/1/1/0/CSA_COUNTERING_CHINA_STATE_ACTORS_COMPROMISE_OF_NETWORKS.PDF>; Cybersecurity and Infrastructure Security Agency, et al., *Enhanced Visibility and Hardening Guidance for Communications Infrastructure* (Dec. 3, 2024), *available online at* <https://www.ic3.gov/CSA/2024/241203.pdf>.

[87] *See* Senator Ron Wyden, *Wyden Releases Draft Legislation to Secure U.S. Phone Networks Following Salt Typhoon Hack* (Dec. 10, 2024), *available online at* <https://www.wyden.senate.gov/news/press-releases/wyden-releases-draft-legislation-to-secure-us-phone-networks-following-salt-typhoon-hack>.

[88] *See* Matt Kapko, *AT&T, Verizon say they evicted Salt Typhoon from their networks*, Cybersecurity Dive (Jan. 7. 2025), *available online at* <https://www.cybersecuritydive.com/news/att-verizon-salt-typhoon/736680/>.

[89] *See* The White House, *On-the-Record Press Gaggle by White House National Security Communications Advisor John Kirby* (Dec. 27. 2024), *available online at* <https://bidenwhitehouse.archives.gov/briefing-room/press-briefings/2024/12/27/on-the-record-press-gaggle-by-white-house-national-security-communications-advisor-john-kirby-38/> ("[A]s we look at China's compromise of now nine telecom companies, the first step is creating a defensible infrastructure.") (statement of Deputy National Security Advisor Anne Neuberger).

[90] *See* Aamer Madhani, *White House Says at Least 8 US Telecom Firms, Dozens of Nations Impacted by China Hacking Campaign*, Associated Press (Dec. 4, 2024), *available online at* <https://apnews.com/article/china-hack-us-telecoms-salt-typhoon-88cabc592dae2fa870772c5ce4ace5ea> ("A top White House official on Wednesday said at least eight U.S. telecom firms and dozens of nations have been impacted by a Chinese hacking campaign…").

[91] *Id*. ("The U.S. believes that the hackers were able to gain access to communications of senior U.S. government officials and prominent political figures through the hack, Neuberger said.")

[92] *See On-The-Record Press Gaggle*, *supra* n. 89 ("Our understanding is that a large number of individuals were geolocated in the Washington, D.C./Virginia area. We believe it was the goal of identifying who those phones belong to and if they were government targets of interest for follow-on espionage and intelligence collection of communications, of texts, and phone calls on those particular phones. So, we believe a large number of individuals were affected by geolocation and metadata of phones; a smaller number around actual collection of phone calls and texts. And I think the scale we're talking about is far larger on the geolocation; probably less than 100 on the actual individuals.") (statement of A. Neuberger).

to harden their networks against a range of cyber intrusions.[93] These actions include accelerating the patching of outdated or vulnerable equipment, updating and reviewing system access controls, disabling unnecessary outbound connections, improving threat-hunting efforts, and cybersecurity information sharing.[94] In addition, the FCC has recently been working more closely with regulators from the U.K., Canada, Australia, and New Zealand to strengthen cooperation amongst these partners to respond to threats against our communications networks.[95]

Yet the impact of these hacks, particularly when combined with other hacks, remains quite serious. The most recent security guidance document released by the U.S. and multiple allied intelligence and law enforcement agencies noted that the Salt Typhoon actors has been operating "globally since at least 2021" and indicated that "[t]he data stolen through this activity against *foreign telecommunications and Internet service providers (ISPs), as well as intrusions in the* lodging and transportation sectors, ultimately can provide Chinese intelligence services with the capability to identify and track their targets' communications and movements around the world."[96] And while that guidance document specifically offered recommendations to close known vulnerabilities in systems built at least three allied providers, the government agencies also noted that they suspected that at least six other vendors may also have been compromised.[97]

At the same time, earlier this year, more than six months after the hack was identified, the FBI sought the public's help in "report[ing] information about PRC-affiliated activity publicly tracked as 'Salt Typhoon' and the compromise of multiple US telecommunications companies, especially information about specific individuals behind the campaign[,]" and specifically noting that if members of the public, "have any information about the individuals who comprise Salt Typhoon or other Salt Typhoon activity, we would particularly like to hear from you."[98] And the U.S. government—apparently having identified at least three Chinese entities involved in the incident[99]—has issued sanctions against one of them.[100]

---

[93] *See Order on Reconsideration*, *supra* n. 85 at 2, 9-10, 13-14 & 17.

[94] *Id*.

[95] *Id*. at 17.

[96] *See Countering Chinese State-Sponsored Actors*, *supra* n. 86 at 5.

[97] *Id*. at 6-7.

[98] *See FBI Seeking Tips*, *supra* n. 82.

[99] *See Countering Chinese State-Sponsored Actors*, *supra* n. 86 at 5 (naming Sichuan Juxinhe Network Technology Co. Ltd., Beijing Huanyu Tianqiong Information Technology Co., Ltd., and Sichuan Zhixin Ruijie Network Technology Co., Ltd. as being linked to Salt Typhoon operations and "provid[ing] cyber-related products and services to China's intelligence services, including multiple units in the People's Liberation Army and Ministry of State Security.").

[100] *See, e.g.*, U.S. Department of the Treasury, *Treasury Sanctions Company Associated with Salt Typhoon and Hacker Associated with Treasury Compromise* (Jan. 17, 2025) ("Additionally, OFAC is sanctioning Sichuan Juxinhe Network Technology Co., LTD., a Sichuan-based cybersecurity company with direct involvement in the Salt Typhoon cyber group, which recently compromised the network infrastructure of multiple major U.S. telecommunication and internet service provider companies. People's Republic of China-linked (PRC) malicious cyber actors continue to target U.S. government systems, including the recent targeting of Treasury's information technology (IT) systems, as well as sensitive U.S. critical infrastructure.")

And yet, in perhaps one of the most stunning revelations to come out of this incident, even as the FCC and White House were calling for significant regulation of American telecommunications companies,[101] the outgoing head of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), published a blog post stating that "CISA threat hunters previously detected the same actors in U.S. government networks."[102] The next day, at an on-the-record event at the Foundation for the Defense of Democracies, the CISA Director stated that while the government had previously detected the Salt Typhoon actors on other federal networks at the time "[w]e saw it as a separate campaign called another goofy name[.]"[103] According to newspaper reports, "CISA's observations didn't prevent Salt Typhoon from attacking the telecom networks en masse, but [the CISA Director] presented the agency's threat hunting and intelligence gathering capabilities as an example of intra-government and public-private collaboration improvements made under her stewardship of the agency."[104]

While all this may make one recall the findings of the 9/11 Commission report, which noted that the U.S. government had both successfully the potential of a major terrorist attack and knew of specific terrorists with visas to enter the United States, but critically failed to share actionable information in a timely fashion with those able to identify and stop those individuals,[105] it also raises important questions about where the responsibility for defending the nation against these types of attacks ought properly lie.

As I previously noted in testimony before another House committee back in 2020, while we've established an entity with the theoretical responsibility for defending the nation in the cyber domain in U.S. Cyber Command, we've never provided it with anywhere near the kind of authorities or resources it would take to actually do that job.[106] And while there may not be a consensus in our nation today on what the government's role in defending our nation's overall cyber infrastructure ought exactly be, the idea that we ought leave our critical infrastructure provider alone to defend themselves against foreign nation-state threat actors—or even worse penalize them when they find themselves unable to stop such actors who come to the fight with

---

[101] *See Chairwoman Rosenworcel Announces Agency Action*, supra n. 84; *see also On-The-Record Press Gaggle*, *supra* n. 89 ("[W]e need to see every member of the — all the FCC commissioners vote to implement the required minimum cybersecurity practices across telecom, because once those are in place, once companies are taking those steps to make their networks defensible, we would feel more confident to say that the Chinese actors have been evicted and can continue to not be able to come in.") (statement of A. Neuberger).

[102] *See* Jen Easterly, *Strengthening America's Resilience Against the PRC Cyber Threats*, CISA (Jan. 15, 2025), *available online at* <https://www.cisa.gov/news-events/news/strengthening-americas-resilience-against-prc-cyber-threats>.

[103] *See* Matt Kapko, *CISA clocked Salt Typhoon in federal networks before telecom intrusions*, Cybersecurity Dive (Jan. 16, 2025), *available online at* <https://www.cybersecuritydive.com/news/salt-typhoon-federal-networks-easterly/737552/>.

[104] *Id*.

[105] *See* National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (July 22, 2004), at 155-59, 181-82, 266-72, *available online at* <https://www.govinfo.gov/content/pkg/GPO-911REPORT/pdf/GPO-911REPORT.pdf>.

[106] *See CISA Clocked Salt Typhoon*, *supra* n. 103.

virtually unlimited resources—is not only unrealistic, it is setting up ourselves to fail every time.[107] Just as we don't expect Target or Walmart to have surface-to-air missiles on the roofs of their warehouses to defend against Russian Bear aircraft dropping bombs in the United States, we ought not expect the same from our telecommunications and infrastructure companies in the cyber domain.[108]

## IV. Considering Effective Responses to Defend America's Communications Infrastructure

This, of course, puts front and center the question of what might be done to address this clear and present threat to the America's communications infrastructure and that of our allies and partners.

First and foremost, we must remember that private sector companies, including those in the the telecommunications and infrastructure sectors, are not primarily in the business of defending themselves against cyberattacks; rather, they operate in order to provide products and services to customers and to generate economic returns from such business. And this is a net positive for our nation and its allies. After all, without these companies, the vast majority of our AI tools and large language models, which rely often rely on connections to cloud infrastructure and access to massive amounts of data and compute, wouldn't be able to operate or service customers large and small across the globe. Without a strong American communications sector, we wouldn't have built, expanded, or maintained the freedom of access to the global information networks that form the Internet. And without American and allied telecommunications and infrastructure companies, we would likely not have seen the massive gains from innovation that have driven the U.S. and world economy for at least the last five decades.

To preserve the value these organizations—and many other private sector entities—provide us, the federal government must partner tightly with industry to enable better cyber defense. This means sharing massive amounts of data (classified and otherwise), providing incentives to obtain and deploy better defensive cyber systems and capabilities, and aggressively imposing costs on adversaries, in appropriate circumstances, to deter the deployment or use of potentially disruptive or destructive capabilities. The fact of the matter is that we cannot cede this critical ground to our adversaries by leaving companies in the telecommunications, infrastructure, and technology sectors alone to defend themselves against nation-state attacks.

---

[107] *See* GEN. Keith B. Alexander, Jamil N. Jaffer, and Jennifer S. Brunet, *Clear Thinking about Protecting the Nation in the Cyber Domain*, Cyber Defense Review 2, no. 1 at 29, 33 (2017), available online at <https://nationalsecurity.gmu.edu/wp-content/uploads/2017/03/CDRV2N1_Clear-Thinking_Alexander_Jaffer_Brunet_032217-1.pdf> ("The fact is that commercial and private entities cannot be expected to defend themselves against nation-state attacks in cyberspace. Such organizations simply do not have the capacity, the capability, nor the authority to respond in a way that would be fully effective against a nation-state attacker in cyberspace. Indeed, in most other contexts, we do not (and should not) expect corporate America to bear the burden of nation-state attacks.").

[108] *See id.*; *see also, e.g.*, GEN (Ret) Keith B. Alexander & Jamil N. Jaffer, *Iranian Cyberattacks Are Coming, Security Experts Warn*, Barron's (Jan. 10, 2020) ("Expecting individual companies to defend themselves against a nation state with virtually unlimited financial resources and human capital does not make sense. Yet today that is our national policy in cyberspace. This is so even though, in every other context, defense against nation-state attacks is the province of the government. We don't expect Target or Walmart to have surface-to-air missiles to defend against Russian Bear bombers. Yet when it comes to cyberspace, we expect exactly that of every American company, large or small.").

One example of providing the right incentives would be to consider—in reauthorizing (and ideally making permanent) the Cyber Information Sharing Act of 2015 (which having expired earlier this year was the subject of a short reauthorization in the recent government reopening deal)—providing the type of liability and regulatory protections that were contained when the original version of that legislation as passed by the House back in 2011.[109] Those protections, which fell out of the legislation negotiated by the House and Senate four years later when it was enacted,[110] are a key example of lining up the incentives between industry and the government and using carrots, instead of the proverbial regulatory stick.[111] Likewise, providing clear authority and direction to provide security clearances and share classified intelligence with the private sector in a manner that allows them to operationalize it, as well as ensuring that private sector entities can go anywhere in the government to share information, as the original legislation did, are also key elements to better collaborating with the private sector on cyber defense. The government cannot expect the private sector to do strong work sharing information within and across sectors, while also maintaining massive silos within the government. We can and should expect better of our federal agencies.

Another key effort that the government ought take up is affirmatively harmonizing existing compliance requirements and regulations across various agencies, and to adopt the collaborative, voluntary approach taken by the FCC, in the first instance. At a minimum, the government ought permit compliance with one set of regulations—ideally those developed in the collaborative manner like that used by the FCC—that the serve as effective compliance with others where the subject matter of the regulation is similar. Likewise, getting unhelpful regulations out of the way and avoiding undermining our own national security policies for political gain by going after our best players—large and small—in the technology industry is critical to avoid. Efforts in recent years to amend longstanding and highly effective antitrust laws that have served our economy well for decades,[112] are a key example of the kind of new policies that would be highly detrimental in the context of the ongoing economic and national security competition with China. These efforts, which target a handful of technology companies based on the nature and scale of their business, are largely driven by policy issues unrelated to innovation or competition.[113] It also sends the

---

[109] *See* Cyber Intelligence Sharing and Protection Act, H.R. 3523, 112th Cong. (engrossed in the House), *available online at* <https://www.congress.gov/112/bills/hr3523/BILLS-112hr3523eh.pdf>.

[110] *See* Consolidated Appropriations Act of 2015, P.L. 114-113, 129 Stat. 2242 ("CISA"); *see also* Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (as passed by the Senate on Oct. 27, 2015).

[111] *See* Jamil N. Jaffer, *Carrots and Sticks in Cyberspace: Addressing Key Issues in the Cybersecurity Information Sharing Act of 2015*, 67 S. Car. L. Rev. 585, 589-98 (2016), *available online at* <https://scholarcommons.sc.edu/cgi/viewcontent.cgi?article=4180&context=sclr>.

[112] *See, e.g.*, American Innovation and Choice Online Act, S.2992, 117th Cong. (2021); Open App Markets Act, S.2710, 117th Cong. (2021).

[113] *See* Bill Evanina & Jamil N. Jaffer, *Kneecapping U.S. Tech Companies Is a Recipe for Economic Disaster*, Barron's (June 17, 2022), *available online at* <https://www.barrons.com/articles/kneecapping-u-s-tech-firms-is-a-recipe-for-economic-disaster-51655480902> ("Conservatives are often worried—sometimes for good reason—that certain social or mainstream media companies might actively seek to suppress or quiet conservative voices. On the liberal side, there are a range of legitimate concerns with technology companies, including the displacement of traditional labor in the new gig economy... Yet rather than tackling these concerns directly by going after the specific behaviors or actions that trouble ordinary Americans, politicians in Washington have chosen instead to vilify some of our most successful

wrong message to startup innovators, namely, that if they thrive and become highly successful, the government might seek to target them for special attention, creating laws just to cut them down to size.[114] The White House has made clear it is on a strong deregulatory path, and action across all of these domains, could help significantly ensure that we are empowering the American private sector to innovate and create and implement better cyber defenses in partnership with the government.

Likewise, we ought work with our allies and partners across the globe—as well as investors and innovators who share our views—to advance American and allied interests, both by deploying capital effectively and ensuring that we don't undermine one another's strongest capabilities in the larger fight against our common adversaries. This also means that we must help our allies across the globe to better protect their own telecommunications infrastructure, which includes sharing information and intelligence ahead of potential threats and coming together to do what we did so effectively here in the United States—removing adversary capabilities, like Huawei and ZTE—from the global telecommunications infrastructure.

It likewise also means that we must lean aggressively forward—both globally and at home—as we look to put in place new technologies like 5G Advanced and 6G, including working collaboratively with across allied governments and industry to get the right international standards in place, including prioritizing allied collaboration on spectrum and on efforts like ORAN, while also protecting historical capabilities, like WHOIS, that have gone—or are going—dark.

The government also ought provide the right incentivizes for industry to build out both domestic and allied communications infrastructure and to invest in the capacity and innovation to deliver advanced technology capabilities globally. To that end, the government should provide tax and other economic incentives for increased private investment in the development of such technologies, the broader deployment of large-scale computing and communications infrastructure to support cloud and edge computing, and the expansion of AI capabilities being made available to U.S. and allied innovators across the globe.

These incentives are particularly important because the security of—and trust in—America's communications infrastructure (and that of our allies) is so central to our success in the larger competition with China. After all, no matter how secure our core technology capabilities themselves are, if we connect them to a weakly defended network, they will no longer be secure.

---

companies and to go after them economically."); *see also* David R. Henderson, *A Populist Attack On Big Tech*, The Hoover Institution (Mar. 3, 2022), *available online at* <https://www. hoover.org/research/populist-attack-big-tech-0>.

[114] *See* Klon Kitchen & Jamil Jaffer, *The American Innovation & Choice Online Act is a Mistake*, The Kitchen Sync (Jan. 19, 2022), *available online at* <https://www. thekitchensync.tech/p/the-american-innovation-and-choice> ("Going after our technology companies, particularly a targeted shot at certain big ones, sends the wrong message to startups and investors alike; it tells them that if you are innovative enough to be successful and grow significantly larger, you may be targeted for different treatment....This undermines not only the companies that are likely to be investing in R&D over the next decade and generating some of the key innovations that will contribute to our national security, it also undermines a central proposition that has created a robust tech ecosystem in this country: take risk, innovate, fail fast and often, and when you succeed, reap the rewards so long as you don't exploit your position to gain unfair advantage."); Evanina & Jaffer, *Kneecapping U.S. Tech Companies*, *supra* n. 86 ("Picking and choosing individual companies to be treated differently than others under our antitrust laws is inconsistent with the heart of our economic system, which Seeks to reward innovation and success, not penalize them.").

If we are to win this competition, therefore, we must ensure that we are properly incentivizing the buildout of these trusted communication capabilities in both the hardwired (including fiber) and wireless domains. Moreover, the government should also work with innovators and investors across the who share our interests to understand key government needs and priorities to develop the innovations and capabilities to address those needs.

Likewise, ensuring that the United States and our allies are able to access the manufacturing capacity and workforce necessary to support a modern technology and communications infrastructure—including consistent access to semiconductors, critical minerals, and other core materials necessary to support major technological innovation—will also be of critical strategic importance to the United States in the coming years, particularly as our competition with China heats up. It is critical that government and industry work together to create the right tax and regulatory incentives to ensure that American and allied companies invest their money here and in allied nations to create much-needed capacity, including in the communications, technology, and infrastructure industries, and to ensure that we have the skilled workers necessary to build and maintain this trusted capacity and capability.

When it comes to addressing lessons learned from the Salt Typhoon hacks and the Volt Typhoon capability deployments, Congress ought consider collaborating with the Executive Branch to appoint an independent third-party commission, taking a page from the successful 9/11, Intelligence Reform, and Cyberspace Solarium Commissions, putting legislators on the panel alongside distinguished private sector and policy leaders to identify key challenges and draft actionable proposals that can actually be enacted by Congress and implemented by the Executive Branch in the near-term.

As noted above, another key element of any effort to push back on adversary operations on our communications networks or to control those networks communications network is to effectively deter those threat actors from taking action in the first instance. While there are those who argue that deterrence doesn't work in the technology domain, the reality is we simply don't practice real, effective deterrence today.[115] We don't talk about the redlines that, if crossed, would provoke a response from the United States, we don't talk about our capacity to respond, we don't talk what a response might look like, and when our communications systems are threatened (or hit), we often simply fail to respond.[116] Even worse, in the rare circumstances when we do respond, we often do so in a fairly limited fashion and without any public acknowledgement or attribution.[117] The problem with this approach is that it undermines any deterrence benefit we might otherwise enjoy.

---

[115] *See* Jamil N. Jaffer, *Statement for the Record, Safeguarding the Federal Software Supply Chain, Committee on Oversight and Accountability*, Subcommittee on Cybersecurity, Information Technology, and Government Innovation (Nov. 29, 2023), at 10, *available online at* <https://oversight.house.gov/wp-content/uploads/2023/11/Written-Statement-Jaffer.pdf> ("[T]he reality is that the United States does not effectively practice deterrence in the cyber domain for a variety of reasons.")

[116] *Id*.

[117] *Id*.

The fact is that if an attacked party is willing to deliver real consequences, and is seen to actually do so, deterrence can in fact work to protect our communications and technology infrastructure.[118]

As such, when it comes to threats to our communications infrastructure, we should be clear about our capabilities, put out a clear declaratory policy on our redlines, and be willing to take swift, decisive, and visible action when those lines are crossed. To do so, therefore, we must authorize, fund, and encourage more forward-leaning efforts by the government to overtly impose substantive costs on our cyber adversaries. It is only through such clear, public, and attributable action can we possibly expect to effectuate real deterrence in this domain.

And finally, the key rubric to apply in this domain, as well as in other key areas of technology across the board, is to apply the traditional American approach to innovation: first, do no harm. In practice, this means allowing innovation to flourish, only having the government intervene in the limited and clear cases, circumstances which ought be extremely rare. American and allied innovation deserves our protection and our support. We ought not, like some of our allies, regulate first and innovate latter. To the contrary, we ought do exactly the opposite.

## V. Conclusion

Such an approach—across all these fronts—is all the more critical when, as now, the United States and our allies are in a massive competition—economic, military, and political—with a near-peer competitor, where technology and innovation is at the heart and soul of the competition. This is a fight we can—and should—win; we just have to get out of our own way and enable our best, most capable actors across the government and industry.

[118] *See* Keith B. Alexander & Jamil N. Jaffer, *Iran's Coming Response: Increased Terrorism and Cyber Attacks?*, The Hill (May 15, 2019) ("While some have suggested that deterrence doesn't work in the cyber domain, the reality is that if an attacked party is willing to deliver real consequences and is seen to do so, deterrence can in fact work.").