LIBERTY BELL PROJECT

Dynamic Competition vs. Predatory Mercantilism

Leveraging Superpower Scale to Build a Trusted Technology Stack

by Clete Johnson and Diane Rinaldo[1]
November 19, 2025

The United States is presently engaged in an undeclared cyber war, playing mostly defense against an aggressive People's Republic of China that is increasingly building a home field advantage leveraged through its aggressive global buildout of technology infrastructure. The adversary combatants are China's military and intelligence services and their cyber criminal proxies, as well as those of China's autocratic supplicants, Russia, Iran, and North Korea. Among these organizations, tens of thousands of highly sophisticated cyber operators wake up every day and go to work against the United States; it is literally their job to infiltrate, steal from, and conduct "battlefield prep" in U.S. and allied critical infrastructure networks, both government and private sector, which constitute the primary domain of this cyber war.

The United States is free and open, dynamic and innovative – and highly vulnerable. Over 15 years ago, Admiral (Ret.) Mike McConnell, the former Director of the National Security Agency and the second Director of National Intelligence, testified to the U.S. Senate Commerce Committee as follows: "If the nation went to war today in a cyber war, we would lose. We're the most connected. We have the most to lose."

We now face the bracing reality of McConnell's prescient admonition from years ago. China is bringing cyber war to us in a vast and multifaceted set of global operations. In addition to conducting newly aggressive offensive operations, the United States needs to adopt a new defense posture at every level of our society, from citizens and communities to companies and local, state, and federal governments. This shift need not and should not be alarmist, but it should meet the urgency of the moment; it must be commensurate with the existential threat that China's predatory technology oppression poses to our free society. All of us in our generation remember doing bomb shelter drills in school. Like in those years of nuclear tension at the height of the Cold War, we should not be paranoid, but we should indeed be prepared.

In the coming decades, there will be many facets of this new posture: operational and technical, scientific and R&D, workforce training and public awareness, military and intelligence, academic research and commercial development. Each of these various needs will draw on – and require changes in – every sector of our economy and society.

This paper does not purport to cover all of these considerations. Instead, it focuses narrowly on one foundational and indispensable element of the domain in which this cyber war is taking place: U.S. communications technology infrastructure, collectively also known as the U.S. "technology stack." As of now, the U.S. technology stack is distinctly diverse and dynamic, still the most innovative in the world, even as China's "national champion" tech behemoths – Huawei

[1] The Liberty Bell Project is a 501(c)(3) non-profit education and training organization whose activities and reports aim to strengthen the infrastructure of our free society; the organization does not conduct advocacy of any kind. The authors draw on decades of experience as senior staff on the House and Senate intelligence committees, in senior leadership roles at the Department of Commerce and FCC, and in the private sector telecommunications industry to provide this perspective on establishing a trusted U.S. communications technology stack.

and ZTE in telecommunications, Alibaba and Tencent in cloud services, Quectel and Espressif in IoT modules, et cetera throughout the tech ecosystem – gain market share and, in some cases, threaten to take over global markets altogether. Almost all aspects of daily life in our free society operate on these networks, so China's technology reach and the coercive power of its espionage and sabotage capabilities constitute an existential threat to our way of life.

* * * * *

With this threat in mind, this paper presents our take on the steps needed to build a full trusted alternative to China's comprehensive "national champions" tech stack.

- Part I illuminates the United States' dynamic superpower status as compared to China's predatory and large – but ultimately self-limiting – autocratic mercantilism.

- Part II explains the critical importance of China-built technology infrastructure to China's cyber war strategy.

- Part III reviews an important predicate step to stopping China's technology threat to the United States: removing Huawei and ZTE equipment and services from U.S. networks.

- Finally, Part IV describes the necessary alternative to the China-built Digital Silk Road of coercive surveillance networks worldwide – a full tech stack established through trusted suppliers operating at scale in U.S. and allied markets – and how to build it.

We argue that this is necessary for the United States' survival as a free society, and that building and maintaining a trusted stack will require significant investment in scale, infrastructure, and cooperation between government and industry – and between the United States and its allies.

We call this "superpower scale." To achieve this imperative, we recommend three steps:

1. Use the AI Action Plan and American Energy Dominance initiatives as models – and as levers – for constructing the trusted tech stack.

2. Leverage the enormous scale and technological capacity of the U.S. and allied markets.

3. Through competition-driven excellence that wins markets through performance, not capture and coddling, deploy the trusted stack throughout our allies, and export it to the markets not yet captured by China.

Part I – Superpower Scale: Competition Beats Capture and Coddling

Unlike China's tech stack, U.S. technology infrastructure is not backed by a brutal authoritarian government that can put the strategic and financial heft of a large nation-state behind a concerted effort to network the world for commercial, espionage, and warfighting purposes. Unlike China's, the U.S. tech stack does not enjoy the start-up benefits of a captured market of well over one billion consumers and protectionist market access restrictions that confer China's "national champions" immediate global scale at the start.

Consider this jaw-dropping statistic: China Mobile's ***5G subscriber base***, with over 550 million users, is almost double the ***population*** of the United States. This figure does not count subscribers for mobile services other than 5G, and it does not include the other two state-owned mobile network operators, China Unicom and China Telecom; combined, China's government-backed "big three" count nearly 1.4 billion subscribers, nearly quadruple the combined subscriber base of the United States' top three, Verizon, T-Mobile, and AT&T. The cloud services market, where U.S. innovation has led U.S.-based companies to win global market share everywhere except for China, is illustrative of China's use of its huge captured domestic market as an incubator for global scale; China blocks world-leading U.S. providers from operating independently in its market, allowing Alibaba, Tencent and others to grow absent competition that is not managed by an China-based entity effectively controlled by China's government:

Cloud Services Leadership by Region

Rank	Worldwide	US	China	Rest of APAC	Europe	Rest of World
Leader	Amazon	Amazon	Alibaba	Amazon	Amazon	Amazon
#2	Microsoft	Microsoft	Tencent	Microsoft	Microsoft	Microsoft
#3	Google	Google	China Telecom	Google	Google	Google
#4	Alibaba	Oracle	Huawei	NTT	Oracle	Salesforce
#5	Oracle	Salesforce	China Unicom	Alibaba	Salesforce	Oracle
#6	Salesforce	IBM	China Mobile	Fujitsu	IBM	IBM

Based on IaaS, PaaS and hosted private cloud revenues in Q2 2024

Source: Synergy Research Group

A similar dynamic is underway in the IoT module market, where only two of the top 10 global manufacturers have operations that are not ultimately controlled by the Chinese Communist Party (CCP). Building on the captured-market-coddled-incubation model that allows China-based manufacturers to conduct predatory CCP-backed pricing and market manipulation worldwide, these companies are poised to seize near total dominance of the global market for these devices, threatening to eliminate all remaining trusted alternative manufacturers. This would mean that in the near future, almost every new connected device in the world would gain its connectivity through a China-made module.

Due to the coercive power arising from the espionage and sabotage possibilities and the basic equipment and services availability inherent in such thorough market saturation, China's capture of these technology markets constitutes an existential threat to the United States and other free societies. China presently has significant advantages in its maneuvering toward this end, especially the sheer size of its captured domestic market. But the United States possesses profound strengths that it can leverage to build a bigger, better, and farther reaching tech stack than China's central planners could envision.

First, the United States is not subject to the self-defeating limits of China's authoritarian and monolithic approach to building networks. The United States has the greatest industrial capacity, the most talented scientists and researchers, the best universities, and the most innovative companies in the world. Its companies begin as start-ups that must innovate, compete, and attract investment and survive a cut-throat market from the moment of inception. Much like

baby sea turtles emerging from eggs in a sandy nest and scrambling across the beach to the ocean to face deadly predators of all types, only a small percentage of these companies will survive to full maturity. To survive and grow, they must earn their market share through dynamism and innovation, persistence and tenacity, pluck and grit; they are not coddled in an enormous captured market that has been handed to them as an incubator in their path to global scale.

And second, the United State possesses a "force multiplier" in scale and market force that is fundamentally different from China in kind, not just degree: the most powerful, dynamic, and well-resourced allies in the world. Allies are willing partners acting on their own initiative to advance their long-term commercial, political, and security interests; they are not supplicants answering to the CCP. Allies act willingly under their own agency for their own purposes, not as conscripts. As the Soviet Union ultimately learned as its empire crumbled, with Warsaw Pact "allies" and Soviet Republics alike fleeing its sclerotic economy and oppressive autocracy, that is a distinction that makes a significant difference in global power. Trusted technology at scale provides a parallel; exceedingly few of the hundreds of millions of people who enjoy the liberties of the United States and our allies would choose to live under China's technology autocracy.

The United States and its defense treaty allies – NATO's 31 other members plus Japan, the Philippines, South Korea, Australia, and New Zealand, all formally postured in defense of the United States, and vice versa – have a combined population of about 1.3 billion people, nearly equaling China's population of 1.4 billion. (Note that China's population is projected to plummet in the coming decades.) But these similar populations are not at all comparable with regard to technology scale, because these U.S. defense treaty allies together constitute the most dynamic, innovative, and productive people in the world, together constituting about 35 percent of the global economy, as compared to China's 20 percent. The paltry economy of China's most powerful supplicant, Russia, constitutes less than four percent of the global GDP, and Iran's and North Korea's economies barely register at all.

Scale matters in technology infrastructure. While the CCP's control over its 1.4 billion people constitutes the mercantilist scale of a huge captured market, the United States has dynamic "superpower scale" along with its defense treaty allies that is actually larger in absolute terms and far more productive and competitive than China's. Leveraging this scale and robust competition, the United States can overwhelm China's mercantilism, which aims to capture global markets through predatory dependencies rather than win in robust competition.

Part II – Technology Infrastructure and China's Art of (Cyber) War

China's approach to building networks is the basis of its cyber war against the United States; the strategy comes straight from Sun Tzu's seminal *Art of War*: "The supreme art of war is to subdue the enemy without fighting."

China has followed this age-old Chinese wisdom in its Belt and Road Initiative, and particularly in its technology component, known as the Digital Silk Road. Through the Belt and Road Initiative, China seeks global influence by developing bilateral "partnerships" – that is, dependencies – in building large-scale physical infrastructure, such as ports, railways, dams, and airports. The exchange is one of both soft power and money, as well as military might. The

loans and partnerships of these projects allow China to gain footholds in strategic international locations, such as seaports of naval military significance. A common criticism of the Belt and Road is China's leveraging multibillion dollar contracts as debt traps. The infrastructure projects are ostensibly commercial investments but they are financed by China, which can manipulate this debt pressure as diplomatic influence. The scale of the Belt and Road Initiative is astonishing and unprecedented, with 147 countries representing two-thirds of the world's population having partnered with or expressed interest in working with China on Belt and Road.

The technology and communications component of Belt and Road is the Digital Silk Road, an umbrella term for China's bilateral efforts to build out infrastructure for sectors including telecommunications, artificial intelligence, the digital economy, cloud computing, smart cities, and more – including the surveillance and sabotage capabilities, Internet censorship, and technology availability that provide China powerful levers of coercion. The Digital Silk Road leverages the market access enabled by other Belt and Road projects to gain competitive and strategic advantages for the Chinese technology stack (including telecom companies) over leading U.S. companies. Much as the bidding process for Belt and Road projects intentionally favors China-based companies, so too are companies like Huawei and ZTE favored in the Digital Silk Road's tech build out, as state subsidies, grants, and tax breaks allow these companies to underbid free market competitors.

The money behind the Digital Silk Road

Chinese state financing for overseas digital infrastructure projects
(announced or committed between 2019 and 2023, selection)

SOURCE	RECIPIENT	AMOUNT (USD MILLION)	DATE	DESCRIPTION
Exim Bank	Ministry of Finance and Economic Development, Sierra Leone	30	2019	Huawei contract for Phase II of National Fibre Optic Backbone Project, laying 690 km of cables
China International Development Cooperation Agency (CIDCA)	Kragujevac State Data Center, Serbia	13	2019	Huawei's AI platform for Serbian e-government services
China Development Bank (CDB)	Turkcell, Turkey	559.9	2019	8-year loan for hardware and equipment procurement from Chinese vendors
Exim Bank	Government of Ghana	177	2020	Huawei equipment for Ghana Rural Telephony and Digital Inclusion Project
Bank of China	Government of Côte d'Ivoire	125.6	2020	Modernization of national police and defense networks and emergency command center
Ministry of Commerce (MOFCOM)	Government of Senegal	Unknown	2021	Contract with StarTimes for Phase II of satellite television program, covering more than 300 villages
Exim Bank	Ministry of Security of Burkina Faso	86.9	2021	Installation of 800 km of fiber optic cables and 900 surveillance cameras by Huawei and China Communications Construction Company (CCCC)
Exim Bank	Government of Benin	40	2021	Phase II of National Broadband Network Project, implemented by Huawei
Unspecified	Egyptian Space Agency	92	2022	Assembly and testing of MisrSat 2 remote sensing satellite by China Aerospace Science and Technology Corporation (CASC)
Sinosure and Citibank	Xtrim TVCable, Ecuador	32	2023	Acquisition of fiber optic equipment manufactured by ZTE
Exim Bank	Government of Uganda	150	2023	Development of national internet infrastructure

Sources: MERICS based on media reports, AidData Global Chinese Development Finance

The above examples of financing and related investments are intended to provide China unprecedented access to influence over global networks and achieve absolute scale advantage over U.S.-affiliated tech stack offerings. In short, following Sun Tzu's advice to "subdue the enemy without fighting," China is building the battlefields on which future wars will have already been won before they are even fought.

China sees technology infrastructure as a strategic – and military – asset. In a 2016 speech, Xi Jinping warned against the dangers of reliance on foreign technology, stating "the control of core technology by others is our biggest hidden danger." Xi also reveals an awareness of the power and influence that comes with China's own exports of technology to foreign partners; the "Made in China 2025" strategy laid out Beijing's ambitious plans to acquire "upwards of 40% of the international mobile communications market by 2025." China issued the action plan for the Made in China 2025 strategy in 2015, the same year that China launched the Digital Silk Road. Furthermore, in 2021, China released a national strategy on international technological standards, which includes influencing the standards development organizations of the communications industry, highlighting China's strategic approach to global communications infrastructure on a multilateral basis.

China's technology strategy benefits from its scale, centralization, and industrial capacity, the playbook it ran to facilitate the rise of Huawei, with subsidies and other strategic support, boosting Huawei's ascent to a global leader in the 5G space. During Huawei's ascendency, China's state-owned banks provided large amounts of capital, a strategy that allowed Huawei to undercut competitor prices and emerge as a market leader. Embedding Huawei's equipment into the communications networks throughout the world was not only commercially beneficial, but of course also beneficial for China's ability to leverage surveillance and security coercion. In 2020, China announced a planned $1.4 trillion in investments over the next six years to boost Huawei and other China-based companies in their efforts to build out 5G wireless networks and install surveillance technologies globally.

Chinese technology stack ambitions are not limited to 5G and communications networks alone. The proliferation of China's offerings in networks worldwide creates dependency and security risks for U.S. technology offerings such as cloud services and AI outside the United States (see the case of Germany, for instance). Even more troubling, China's monolithic global technology stack approach uses connectivity as an entry point to subsequently push out and displace U.S. cloud and AI solutions in non-U.S. markets.

This is particularly concerning given the relationship between the CCP and China-based companies. For instance, Huawei is nominally a private company, but the national security laws of China's authoritarian regime require reporting and also forms of active operational assistance to security authorities upon request. This eviscerates any concept of private-sector network security and opens all Huawei-built networks to CCP probing, and perhaps even control, at the whim of the Chinese intelligence services.

China's multifaceted cyber threat, which of course predates and goes beyond the Digital Silk Road, is further facilitated through China's technology stack supply chain – that is, any and every company ultimately controlled by the CCP. This threat is singularly unique to China's mix of technology prowess and authoritarianism. Rather than needing to conduct a sophisticated cyber operation to hack into or activate a "back door" compromise in a system, China's intelligence services can simply gain access through the "front door" of Huawei's – or any CCP-influenced company's – networks. In contrast, the United States and its allies require the vetting of an independent judiciary to obtain a warrant to intercept private communications or to direct a security operation such as a botnet takedown. Given the scale of the Digital Silk Road, this is a

critical security vulnerability of global proportion. This problem will worsen as China continues to combine government subsidies, access to cheap and vast amounts of capital, and ongoing state support to drive other non-CCP-controlled suppliers out of business.

The buildout of communications infrastructure on China-made technology introduces risk throughout the technology stack. Manufacturing and distribution processes are particularly vulnerable to interference by sophisticated bad actors through the inclusion of hardware susceptible to remote access or malignant software activity on connected devices. Further, post-sale targeted malware embedded through firmware updates or "human intelligence" operations also pose significant risks. These cyber-supply chain espionage or sabotage operations are conducted by adversary intelligence services – not just China, but also Russia, Iran, North Korea, and criminal proxies of these governments – and such operations are exponentially more simple and their goals more easily achievable if the technology in question is made, deployed, or maintained by companies that are subject to CCP control in the first place.

It is not a question of *whether* China's intelligence services would leverage such capabilities and vulnerabilities; of course they would. They have done so already in multiple operations and will continue to do so; this is what they do. China's cyber operations, especially against the United States, are brazenly voracious and aggressive. The extraordinary reach of China's tech and telecommunications manufacturers into the global communications market provides innumerable opportunities for China to leverage this strategic advantage through cyber and human operations.

Even without having fully built out the global technology battlefield, China's aggression in cyberspace has already been extremely problematic for long-term U.S. interests. In the past several years, several instances of China's advanced persistent threats have emerged, revealing exploitations that have realized these very concerns. In 2020, hackers inserted malicious code into the Orion software platform used by thousands of public and private organizations in the SolarWinds incident. While the hack was primarily suspected to be the work of Russia-affiliated actors, China reportedly also piggy-backed on the compromise. The malware was distributed through legitimate software updates, giving attackers deep access into the networks of U.S. federal agencies, critical infrastructure, and Fortune 500 companies. In 2024, the FBI announced certain actions it had taken under court-authorized operations to disrupt China's "Volt Typhoon" campaign of surreptitiously pre-placed malware in U.S. critical infrastructure for future cyber disruption capabilities. Also in 2024, multiple major U.S. communications providers were affected by China's "Salt Typhoon" advanced persistent threat activities. The attackers gained access to network infrastructure, embedding themselves in core systems, physical switches, routers, and telemetry systems, and wiretapping systems used by U.S. law enforcement to conduct court-authorized surveillance.

While initiatives like the Digital Silk Road have given China a head start on building the underpinnings of the global communications network as a foundation for a global Chinese technology stack, the time is still ripe to provide an alternative through the development and export of an American trusted full stack offering.

LIBERTY BELL PROJECT

Part III – The Necessary Predicate Step: Finishing a Trusted Tech Stack at Home

The first, and in some ways the easiest, step to address this problem is to minimize the presence of untrusted China-manufactured equipment in U.S. networks, especially from suppliers with global reach like Huawei and ZTE. Large U.S. network operators have avoided these untrusted suppliers through the vast bulk of U.S. network infrastructure; accordingly, and with a strategy that could have been written by Sun Tzu, the CCP sought to embed Huawei and ZTE in vulnerable small rural network operators.

For two decades – and particularly the last eight years dating back to early in the first Trump Administration – policymakers across the U.S. government have taken bipartisan steps to address national security threats posed by companies subject to control by foreign adversaries (namely China) within critical infrastructure supply chains. The FCC has played a central role in this effort with its Supply Chain Reimbursement Program driving a widespread shift in U.S. telecommunications supply chains away from China-based suppliers such as Huawei and ZTE.

This reimbursement process developed via iterative rulemaking and various legislation and was implemented with only partial funding amid the Covid-19 pandemic, presenting significant challenges and sometimes insurmountable burdens on small American telecommunications providers. The Program focuses on recipients of the FCC's Universal Service Fund (USF), whose providers serve the hardest-to-reach areas in the United States with very little margin in their operating budgets. Heightened supply chain and labor demands and novel administrative burdens imposed by this new Program, along with the terrain challenges that accompany broadband deployment in these areas, have placed unprecedented pressure on our nation's smallest network owners and operators to maintain critical services – all amid years of regulatory and political uncertainty and complex geopolitical tensions.

The Trump Administration is now poised to break through these obstacles and complete the job begun in the first Trump Administration. Late last year, Congress approved an additional $3.08 billion in the FY2025 National Defense Authorization Act (NDAA) to fully cover eligible estimated expenses under the Supply Chain Reimbursement Program, reiterating that this effort remains a bipartisan policy priority. Finally, in April 2025, the FCC under Chairman Brendan Carr announced that it had finally gained access to all the funding it needs for reimbursing the replacement of equipment from Huawei and other untrusted suppliers on the Covered List.

With full funding finally in place and available for reimbursement, the Trump Administration and the Carr-led FCC see completing Rip and Replace as a key goal for their aim to cut through red tape and make government work. Completing this basic task – an indispensable step toward securing U.S. networks – is now years overdue. As Chairman (then Commissioner) Carr noted five years ago:

> "We cannot treat Huawei and ZTE as anything less than a threat to our collective security … Communist China intends to surveil persons within our borders and engage in large-scale, industrial espionage. Nothing short of prohibiting subsidized Huawei and ZTE gear from our networks could address this serious national security threat."

Accordingly, the Trump Administration and the Carr FCC are undertaking or considering the following steps to expedite this process:

- Streamlining administrative processes to speed disbursements;
- Incorporating private sector processes for reimbursement;
- Reimbursing financing costs and allowing for advanced financing; and
- Fast-tracking siting and permitting.

In 2012, the House Permanent Select Committee on Intelligence issued its seminal report on the threat that Huawei poses to U.S. security and the first U.S. government restrictions on Huawei were enacted in the Public Safety and Spectrum Act (which, among other things, created the FirstNet interoperable first responder broadband network).[2] Since then, multiple Administrations, Congresses, and FCCs have taken steps to address this threat. Since 2018, these steps have included attempts to rid U.S. networks of Huawei and ZTE equipment.

The Trump Administration and the Carr FCC are now poised to finish this job rapidly. Doing so is long overdue. But while indispensably necessary, "rip and replace" is only the predicate first step to constructing an alternative trusted stack. Beyond the connectivity infrastructure that the CCP sought unsuccessfully to embed in the United States through Huawei and ZTE, China's autocratic technology march continues domestically in the United States, from data apps such as TikTok to IoT enablers (Quectel) to drones (DJI).

Part IV – Building a Trusted Technology Stack

The United States must build a trusted stack as if the future of its free society depends on it – because it does. The first Trump Administration recognized this fact in its early efforts to build trusted networks overseas that went beyond the connectivity layer to cloud service and apps; now, in the second Trump Administration, the importance of this comprehensive full tech stack is further manifest in the rise of modern AI systems, most of which are fundamentally dependent on robust, high-speed connectivity infrastructure.

Consider that large language models require massive data transfers between distributed computing resources; real-time AI applications demand ultra-low latency connections; machine learning systems continuously exchange training data, model parameters, and inference results across networks spanning continents. This connectivity dependency creates a critical attack surface that adversaries can exploit to compromise AI systems, steal intellectual property, conduct espionage, or disrupt critical operations. The connectivity layer of the tech stack encompasses multiple components: telecommunications equipment, fiber optic cables, satellite communications, network switching hardware, and the software that manages data flows. However, mobile networks and 5G infrastructure represent particularly critical vulnerabilities in the AI ecosystem. 5G networks, with their ultra-low latency capabilities and massive device connectivity, are becoming the primary enablers of edge AI applications, autonomous systems, and Internet of Things (IoT) deployments that depend on AI processing.

[2] The Public Safety and Spectrum Act of 2012, enacted as Title VI of the Middle Class Tax Relief and Job Creation Act of 2012, Pub. L. No. 112-96 (2012), placed certain implicit not-by-name restrictions on Huawei's participation in processes that established FirstNet.

A. What Is a Trusted Supplier?

Determining what constitutes a "trusted supplier" is critical to building and maintaining a secure technology stack. Trustworthiness must be assessed across multiple dimensions, including political and governance context, business practices, cybersecurity risk mitigation, and the role of government in setting standards. Frameworks developed by the Center for Strategic and International Studies (CSIS), the National Institute of Standards and Technology (NIST), the United Kingdom, and the European Union provide a comprehensive basis for evaluating suppliers. The Prague Proposals for 5G security first captured these trust principles as a formal statement from the U.S. and dozens of allies in May 2019 during the first Trump Administration.

These principles boil down to a simple question: Can the technology in question be trusted to serve its user's needs, or is the technology subject to manipulation for other interests?

In this simple analysis, suppliers are more trustworthy when they are governed under the laws of countries with strong market democratic and rule of law traditions. This includes separation of powers, competitive elections with viable opposition parties, media freedom, and demonstratable respect for the rule of law. A supplier's adherence to international norms, both commercially and in terms of human rights, further enhances its trustworthiness. Transparent business practices that can be independently verified are another cornerstone of trust. A supplier that maintains a clear governance structure, is publicly traded or otherwise subject to robust regulatory oversight, adheres to international accounting standards, and respects intellectual property is inherently more trustworthy. Conversely, companies with opaque ownership structures, lack of financial transparency, or direct state ownership present heightened risks and should be treated with caution.

Below we describe key criteria of trust, namely, risks emanating from government influence, ownership and control, financial influence, and political influence. Each of these criteria should be seen as indicators – not formulaic or determinative alone, but rather a measurement tool for evaluating the risk that a supplier is subject to influence that could lead to an introduced vulnerability in or through its supply chain.

Generally, China-based companies fail the trust evaluation on almost all counts, whereas most companies that operate under the laws of the United States and its allies meet all these criteria.

Legal structure of country of headquarters. A supplier headquartered in a specific nation state will of course be subject to the laws of that nation state. Subsidiaries to that supplier, established outside that state, will arguably also be indirectly required to comply with such laws, because oflegal requirements or internal directions from headquarters. The jurisdictions applicable to the supplier's headquarters is an important external factor to assess. Further, certain parts of a supplier's operations or parts of its supply chain may be subject to different jurisdictions. It is therefore important to determine if foreign jurisdictions are applicable to essential parts of the supplier's operations or sourcing structure. This is particularly relevant to China's National Intelligence Law which imposes broad legal obligations for entities and persons to cooperate with national intelligence agencies in intelligence collection. If a supplier is subject to such laws, there is obviously an increased risk that the supplier is, or may in the future become, influenced

and legally required to participate in such intelligence gathering on behalf of China. Such intelligence gathering may entail covert interception of communications from a network. Thus, a security assessment should also focus on the legal framework in foreign states that have jurisdiction over the supplier, such as where the supplier or its parent company is headquartered in that foreign jurisdiction, to verify whether it is, or could become, legally obliged to participate in national intelligence gathering.

The ownership structure of the supplier (including adversary government ownership). A foreign state owner would presumably be able to directly influence the supplier's decision-making, both with respect to commercial decisions such as price undercutting to certain customers or sectors which are of interest to state policy, and with respect to covert activities, including cyber espionage. The presumption that adversary government ownership and/or voting authority may influence a supplier's decision-making, and that it therefore constitutes a security risk, is well established in legal regimes such as the U.S. CFIUS review process. Government ownership alone might not be a high-risk factor if a company is subject to securities laws and regulatory oversight by authorities in different jurisdiction, which ensure transparency and independency of business decisions. However, if the supplier is state-owned, and also subject to a legal regime in that same state which requires the legal entity or its employees to engage in a state's intelligence gathering, an authority may view the two factors in combination and determine that collectively, they make out a higher risk for government influence.

Control over the supplier. The ability of external interests to exercise control of the supplier is a relevant factor even if there is no formal equity or ownership at stake. The ability to control an entity will depend on several factors including the type of entity, its legal status, governance structure, and the legal framework of the jurisdiction where the entity has its seat. Generally, U.S. and allied governments look to the following criteria for determining control over an entity:

- the power to appoint or remove a majority of members of the administrative, management or supervisory board;
- controlling the voting rights of an entity, for example through a shareholder agreement, or by having the legal right to do so either through agreement or law; or,
- to exercise influence over the entity and have the right to use the entity's assets.

Financial influence over the supplier. Financial considerations, of course, may affect the supplier's decision-making. A supplier that has access to or is dependent on state funding or state-backed funding, will likely be more vulnerable to political influence and pressure than suppliers that have acquired financing from independent market-based financial institution.

Political influence over the supplier. Objectively verifiable criteria include legal or formal requirements that political representatives are part of an administrative or management board or council of the supplier. For example, if there is a formal requirement that the chair of the board also holds the function of representative of a political party, there is arguably significant political influence over that entity. Such formal requirements could be set either in legislation, by way of state directives, or by informal requirements such as by introducing political influence in the articles of association of the entity. Thus, even companies that are not formally state-owned will, in such regimes, be subject to significant political influence.

B. Ensuring That a Trusted Stack is a Secure Stack

A trusted supplier with poor technical security is a problem, just as is a technically secure supplier that lacks trust. Expertly vetted, deployed, implemented, maintained, and operated solutions must extend across the entire network environment. This includes hardware and software components, cloud infrastructure, third-party services, and the broader security posture and operations that tie everything together. Ensuring each layer of this environment is rigorously managed provides the foundation for resilience and adequate security posture. To be clear, a trusted stack is more than an assessment of autonomy of suppliers — trusted stack needs to be secure and therefore, technical verification and tests are also needed.

This approach goes beyond Reagan's famous arms control principle of "trust but verify" by embracing the technical concept of "zero trust architecture" in which a stack maintains security by assuming the possibility of compromise and ensuring rapid remediation. Together, these measures ensure that reliability, security, and scale are not one-time achievements, but ongoing practices embedded into network operations.

NIST has emphasized that supplier trust is not a static designation but a dynamic, lifecycle-based process. Evaluations must extend beyond prime contractors to include sub-tier suppliers, software vendors, and service providers. Supplier trustworthiness should be monitored across the entire system lifecycle, from acquisition and development to operations and decommissioning. Changes in ownership, financial health, or security posture can alter risk and must be accounted for. NIST also highlights the importance of embedding enforceable trust criteria into contracts, including requirements for incident reporting, third-party audits, and secure development practices.

The Trusted Computing Group emphasizes the need to build trust from the bottom up, beginning with hardware and extending through firmware, hypervisors, operating systems, and applications. This ensures that protections are in place from the moment a system boots, unlike software-only solutions that leave critical windows of vulnerability during initialization. By embedding trust at the hardware level, this approach establishes a stronger foundation for resilience across the broader ecosystem.

For instance, one major trusted supplier's cyber network security framework provides a useful lens for conceptualizing the trusted stack, emphasizing that security must be integrated at every stage of the technology lifecycle. At the operations level, the framework highlights the importance of secure operational procedures, ongoing monitoring of system performance, proactive vulnerability management, and the ability to detect, respond to, and recover from attacks. At the deployment stage, networks must be designed with resilience in mind, incorporating secure configurations, hardened parameters, and architecture that anticipates evolving threats. The vendor product development process further reinforces trust by requiring secure hardware and software components, rigorous development practices, and strict version control with timely, secure software updates. Finally, at the foundation of the stack, the telecommunications standardization process ensures that secure protocols, algorithms, and storage practices are consistently applied across the ecosystem.

Again, "zero trust architecture" forms another cornerstone of this model. As networks become more complex, integrating cloud infrastructure, artificial intelligence, and the Internet of Things, the attack surface expands significantly. Each of these elements introduces new vulnerabilities and entry points for adversaries. Zero trust responds by assuming that an attacker may already be inside the network. The goal is therefore not simply to defend the perimeter, but to secure individual assets, block unauthorized access, and prevent lateral movement. Key practices include encryption of traffic, deployment of network sensors, and segmentation of data. By assuming that the first line of defense will eventually be breached, zero trust prioritizes rapid detection, containment, and damage mitigation.

This approach is reinforced by NIST Special Publication 800-207, which provides the U.S. government's framework for zero trust architecture. NIST emphasizes that no implicit trust should be granted based solely on network location; instead, every access request must be continuously authenticated and authorized. By focusing on protecting individual resources rather than relying on perimeter defenses, the NIST model complements industry adoption and underscores zero trust as a systematic, scalable response to modern network complexity.

Promoting process-based supply chain security standardization is a critical step. One industry-led benchmark is SCS 9001, described as a Global Cybersecurity and Supply Chain Security Standard for Today's Evolving Threat Landscape. This standard sets rigorous requirements for supplier processes, cybersecurity practices, and operational resilience. It is designed to ensure that products and services entering a network ecosystem have been verified against strict criteria for integrity and security. Its process and trust-related requirements are so stringent that suppliers based in China and other foreign adversaries would be unlikely to qualify, making it an effective, industry-led filter against systemic risk. Widespread adoption of a supply chain security standard of this kind would offer practical and strategic benefits for the trusted stack.

Due to the technical threat capabilities that the CCP maintains, purely technical means to bolster trust are inherently limited. Again, sophisticated adversary intelligence services like China's are capable of espionage or sabotage operations through remote access, firmware updates, or targeted HUMINT-enabled SIGINT. On trusted infrastructure, malicious cyber operations require a sophisticated plan to break into the network or to activate a "back door," but for China's intelligence services, a CCP-dependent network allows government officials to gain access simply by requirement – effectively sidestepping the need to break in or create a back door and instead simply start their operation through the front door.

C. How Can the United States Build a Trusted Stack?

The U.S.-China digital tech stack competition is driving technological decoupling in critical sectors, creating parallel supply chains and innovation ecosystems. The competition will likely intensify as both countries seek technological self-reliance in critical areas while maintaining competitive advantages in global markets. The ultimate outcome will depend on each nation's ability to maintain innovation leadership, secure reliable supply chains, build effective international partnerships, and adapt to rapidly evolving technological landscapes. This competition will fundamentally reshape the global technology market and determine the technological foundation of the emerging new world order.

AI has not only become central to America's economic competitiveness and national security but is the central focus of the intensifying geopolitical competition with China. It is therefore imperative that United States adopt a comprehensive approach to securing its AI technology stack, as is evidenced by the Administration's AI Action Plan and the Commerce Department's recent Request for Information for promoting the export of a trusted AI technology stack. The U.S. government has prominently focused on securing AI chips, algorithms, data centers, and cloud services, as well as the electric power to enable AI. This is indispensably important, but one critical vulnerability remains largely overlooked: the connectivity layer that enables AI systems to function, communicate, and scale.

Establishing trusted suppliers in the connectivity infrastructure in the U.S. domestic market, while largely achieved as described in Part III above, is not enough alone. To deploy a trusted U.S. AI and cloud stack, and to push back on China's monolithic approach to building a Chinese global technology stack, it is also essential to devise a trusted full technology stack approach internationally throughout the "superpower scale" market.

The security of U.S. AI and cloud technology depends critically on the integrity of the connectivity infrastructure that enables AI and cloud systems to function and scale. As AI becomes increasingly central to economic competitiveness and national security, the United States must extend its focus beyond chips and algorithms to encompass the full technology stack, including trusted suppliers in the connectivity layer. The global race to deploy 5G infrastructure creates path dependency to 6G. If untrusted suppliers capture significant market share in 5G deployments, they could establish dominant market positions in 6G that become difficult to dislodge, potentially creating long-term dependencies on potentially compromised infrastructure that will support decades of AI innovation.

This imperative requires immediate attention and coordinated action across government, industry, and international partners. The cost of inaction, measured in compromised national security, economic vulnerability, and technological dependence on potentially hostile actors, far exceeds the investments required to build a secure, trustworthy connectivity ecosystem for America's AI future. The window of opportunity to establish these protections is narrowing as AI deployment accelerates and global connectivity infrastructure continues expanding. Swift, decisive action to prioritize trusted suppliers in the connectivity layer internationally represents not just sound policy but an essential investment in America's long-term security and prosperity in the age of artificial intelligence.

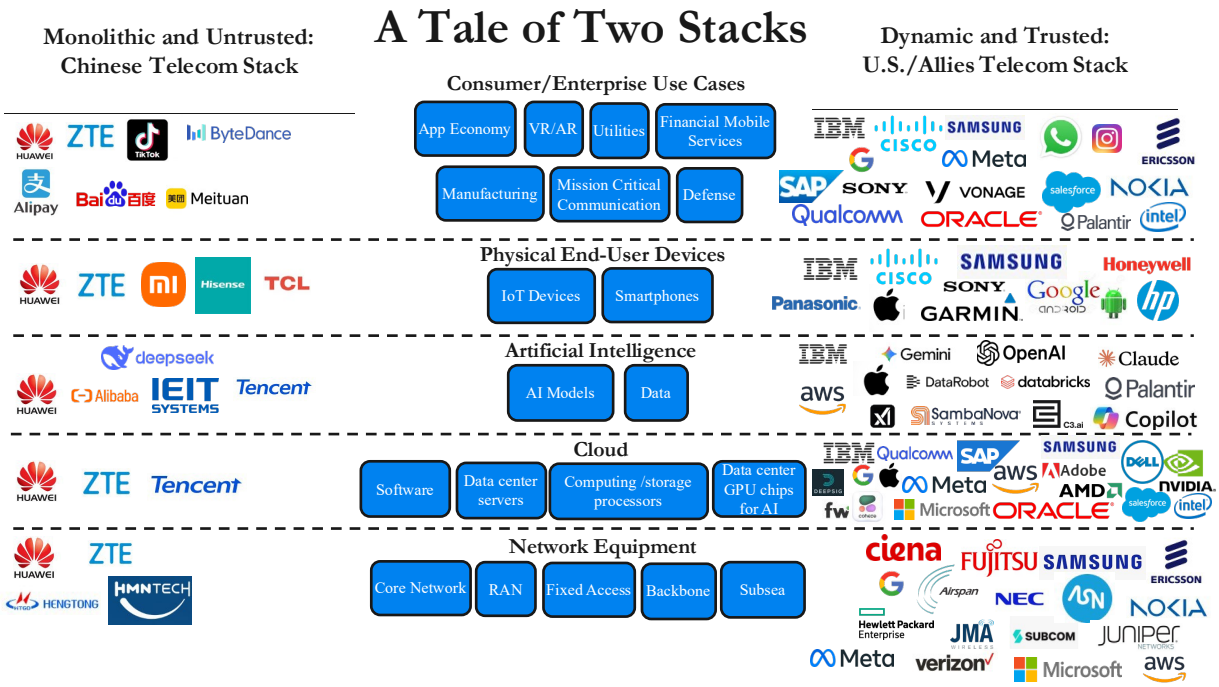
Building and maintaining a trusted stack will require significant investment in scale, infrastructure, and cooperation between government and industry, and between the United States and its allies. We recommend three general steps:

1. Use the AI Action Plan and American Energy Dominance initiatives as strategic models, and also as industry levers, to construct the trusted tech stack.

2. Leverage the enormous scale and technological capacity of the American and allied markets to achieve cost efficiencies and broad market reach.

3. Deploy the trusted technology stack throughout our allies, export it to the addressable markets not yet captured by the CCP, and promote trusted technology stack policies among all allies and partners to ensure that untrusted suppliers are phased out from and not deployed in critical infrastructure.

Trusted connectivity is an integral part of the trusted stack, but as the Trump Administration has recognized in its AI Action Plan, the trusted stack must ensure that all elements of digital infrastructure, from connectivity to cloud to AI capabilities to devices to consumer and enterprise use cases. Below, we focus on mobile and RAN as especially illustrative of the possibilities for building a trusted stack, but we note that a broader conception of the stack is imperative.



First, the AI Action Plan lays out several key steps to strengthen AI infrastructure. These include deregulating AI by removing barriers to innovation and adoption, fast-tracking data center infrastructure permitting to accelerate the buildout of high-performance computing capacity, and promoting the export of the U.S. AI technology stack, thereby fostering international trust and interoperability. In parallel, the Administration has tied AI development to defense and infrastructure modernization. A proposed $300 billion federal spending package is directed toward AI-enabled defense and homeland security systems, including drones, sensors, and surveillance platforms. These investments are designed to ensure that the trusted stack is not just a commercial framework but also a national security imperative, supporting critical infrastructure across the defense sector.

Energy management and resiliency should form another critical lever of the trusted stack strategy. The Department of Energy ("DOE") has partnered with the private sector to accelerate grid modernization efforts, including on load forecasting for AI infrastructure and the strategic

siting of data centers. As part of the AI Action Plan, the Administration is also fast-tracking permits for power generation to support the growth of data centers and telecommunications hubs. In addition, DOE-FCC coordination has expanded to include joint programs for infrastructure resilience, such as redundancy planning for base station energy and the deployment of long-duration energy storage.

Likewise, powering next-generation communications networks is central to the trusted stack. High performing, energy efficient networks – including, for instance, Open RAN and edge systems – increasingly depend on modular energy solutions. Major equipment providers have begun to bundle low-power hardware with off-grid solar, backup batteries, and microgrid-ready systems to ensure continuous uptime and build trust in deployed systems. For instance:

- (Qualcomm) Gridspertise Quantum Edge Device ("QEd"): an edge AI platform that virtualizes substation grid functions with strong cybersecurity;
- (Qualcomm/Lantronix) SmartLV Edge Gateway: a rugged, secure, AI-enabled LTE/5G gateway for resilient substations;
- (Samsung) Green Site Power Solution: modular solar-plus-battery systems with smart controllers for energy-resilient RAN sites;
- (Samsung/Verizon) AI Energy Saver Manager ("AI-ESM"): AI-driven energy orchestration across live RAN deployments, achieving substantial power savings;
- (Ericsson) Energy-Smart 5G Site: coordinates multiple energy sources through intelligent load management techniques such as peak shaving and demand response;
- (Ericsson) Green Energy Site Solutions: offers pure solar and hybrid solar-grid configurations for rural 5G deployment;
- (Ericsson) Site Energy Orchestration Platform: an AI-driven interface that links RAN systems with energy grids, enabling operators to optimize energy use across multiple sites and even act as 'virtual power plants' in energy markets;
- (Nokia) Private Wireless Connectivity for Microgrids: deploys secure, industrial-grade private wireless networks to ensure reliable, real-time communication between microgrid controllers and distributed energy assets; and
- (Nokia) Edge Communications for Renewable Energy Facilities: delivers private LTE/5G solutions that empower wind and solar farms with robust, low-latency communication for asset monitoring and automation.

The second step in building a trusted American technology stack is to leverage the enormous scale and technological capacity of the U.S. and allied markets. The United States benefits not only from its own industrial and innovation base, but also from deep integration with ally-headquartered companies that operate extensively within the U.S. economy. For instance, large network infrastructure firms such as Ericsson, Fujitsu, NEC, Nokia, and Samsung, which are headquartered in defense treaty ally countries and maintain enormous U.S. operations, facilities, and employee bases that make them significant contributors to the U.S. technology landscape. For instance, Samsung's North American footprint includes more than 25,000 employees;

Ericsson's 12,000; and Nokia more than 8,000. Similarly, Japan-based firms such as Fujitsu and NEC employ nearly 4,000 and 3,000 individuals, respectively, in North America, anchoring their role as allied suppliers with deep ties to the U.S. economy. These companies have large brick-and-mortar manufacturing, research and development facilities in the United States, demonstrating that they are deeply embedded into the U.S. and allied industrial base, and thus, integral to the construction of a resilient and trusted stack.

Alongside these companies, U.S.-headquartered companies such as Cisco, Intel, Oracle, Qualcomm, Cisco, Intel, and dozens of others (e.g., Airspan, Cohere, DeepSig, Federated Wireless, JMA, etc.) compete in the same markets and remain indispensable to U.S. technology leadership. Together, these companies represent the backbone of a trusted technology marketplace and must be fully integrated into the American trusted stack. Their participation ensures that the United States maintains both the diversity and scale of suppliers necessary to compete globally in the next generation of networks and communications technologies.

The importance of this approach was stated in comments from the Open RAN Policy Coalition to NTIA in the context of promoting Open RAN, as the Coalition argued that NTIA should "promote a robust and trusted global market that leverages U.S. innovation." In particular, the Coalition emphasized that the interests of U.S. companies, workers, and national security are best served by a robust and resilient trusted globally scaled market in which American and allied firms compete to develop and sell components and software across all layers of the stack. Such a market would not only enhance the diversity of supply for U.S. operators but also promote secure networks in allied countries, advancing broader U.S. security goals. Only a multinational, diverse vendor base will have the scale and capacity to meet demand in both the United States and allied markets. The Coalition highlighted that Open RAN deployments, trials, or testing facilities already span markets representing $55 trillion in GDP and 3.3 billion people – nearly 59 percent of the global GDP and 43 percent of the global population – and stated that the addressable market for open and interoperable RAN solutions is even larger still.

Taken together, these arguments reinforce that the trusted stack must draw on the capabilities of both U.S.-headquartered firms and multinational allies, harnessing their collective scale to compete with untrusted vendors.

The third step, leveraging competition-driven excellence that wins markets through performance not capture, is deploying the trusted stack throughout our allies, and exporting it to the addressable markets not yet captured by the CCP. Through the AI Action Plan and broader diplomatic initiatives, the United States is already working to extend its technology stack, including secure communications hardware, AI-enabled infrastructure, software-defined networks, and cybersecurity protocols, to allies and strategic partners. The objective is to establish a common baseline of trusted, interoperable systems that reduce reliance on untrusted vendors, particularly those based in China and other foreign adversary jurisdictions.

Successfully deploying this trusted stack at a global scale will require sustained investment in domestic infrastructure, incentives to support secure and resilient manufacturing, and close coordination with allies. We need both smart export controls that solve for national security concerns – namely, not helping China's armament through U.S. technology – and also allows

trusted companies to compete and deploy globally. Only by combining domestic capacity with U.S. and allied scale can the United States ensure that its trusted stack becomes not just a national framework, but the international benchmark – at dynamic superpower scale.

Conclusion: The Meaning of 1989 for the Technology Stack

In 1776, the United States declared its independence from a monarch's tyranny; the same year, Adam Smith published his world-changing critique of mercantilism, *The Wealth of Nations*, promoting the economics of robust competition over the economics of imperial hoarding. The sweeping economic, technological, social, and political changes that the United States and its allies have ushered in through the nearly 250 years since 1776 are now directly relevant to the existential need to build a trusted technology stack.

Consider 1989, the year in which free societies based on the rule of law, competitive markets, and representative governance began to achieve what at the time appeared to be the final defeat of autocracy. Free people in Berlin took down the Wall that for decades had kept East Berliners captured in illegitimate oppression; likewise, free people in the rest of East Germany and also in Hungary, Poland, Czechoslovakia, and Romania, began to throw off the cloak of the Iron Curtain. Within a few years of 1989, two centuries of competitive market democracy had defeated monarchical, fascist, and, finally, communist autocracy – apparently proving to be the most effective, dynamic, and powerful form of human governance. Prominent scholars said it was the End of History.

But in China, things moved in a dramatically different direction in 1989. The still quite young Chinese Communist Party autocracy – which in its then-forty years in power had brought the Chinese people mostly misery, death, and impoverishment through the catastrophic Great Leap Forward and subsequent Cultural Revolution – appeared in August 1989 to be going the way of the Soviet Union's autocracy. However, murderous tanks and gunfire defeated free society's stirrings in Tienanmen Square, and the CCP has ultimately succeeded the Soviet Union as the world's despotic empire. Along with its weak but dangerous autocratic supplicants – Russia, Iran, and North Korea – China seeks a new world order based on oppression, surveillance, and information control.

Almost forty years after the atrocities of Tienanmen Square, the CCP now celebrates its nearly eight decades in power with an alliance of autocratic regimes that in any future conflict will rely not only on traditional military hardware but also network infrastructure. Thus, constructing, deploying, and exporting a trusted technology stack is imperative. This is not only a matter of commercial vibrancy – although it is certainly that – but also a matter of national security. The tech stack is core infrastructure that provides the foundation for and indeed shapes our society. As China's influence in global communications networks grows for its own strategic purposes, the autocratic threat to the U.S. and allied free societies increase in direct proportion.

This conflict is upon us, and the time is now to strengthen our networks and construct a trusted alternative tech stack for U.S. and allied use. China has spent a decade embedding its technology in networks around the world, and combatting this "battlefield prep" will require first removing the equipment of Huawei and ZTE, and building out the trusted stack. The United

States will not and need not have a Belt and Road Initiative or Digital Silk Road or otherwise manipulate the markets with vast amounts of capital and subsidies; this is not the U.S. approach. Instead, the United States should harness our and our allies' innovation and market power to develop and deploy the trusted stack by investing at scale in manufacturing, infrastructure, and cooperation between industry and government. In securing our networks through dynamic and competitive superpower scale, we secure our free society – and flipping Sun Tzu's wisdom, we thwart our adversary's attempt to subdue us without fighting.