April 30, 2026
Joseph E. Lin
Co-Founder and CEO, Twenty Technologies, Inc.
Testimony Before the U.S.-China Economic and Security Review Commission
"Taking a Bigger Byte: China's Expanding Strategy for Data Dominance"

Introduction

The People's Republic of China (PRC) has undertaken a state-directed systematic initiative for converting data into intelligence advantage, economic leverage, artificial intelligence (AI) advancements, coercive influence, and wartime decision superiority. This challenge is broader than cyber espionage in the traditional sense. In the last five years, the threat has evolved from already serious cyber-enabled espionage and intellectual-property theft into an integrated model that combines mass data acquisition, long-duration persistence in high-value networks, compromise of telecommunications backbones, exploitation of contractor and data-broker ecosystems, and pre-positioning in critical infrastructure for potential coercive or disruptive use during a crisis.

At a strategic level, Beijing treats data not as a neutral byproduct of commercial life but as an input to state power. In the PRC system, the distinction between "commercial" and "military" data is often less meaningful in practice than it appears in law or in ordinary market analysis. Telecommunications metadata, logistics records, health and genomic data, cloud telemetry, financial signals, and consumer location can all acquire military significance once fused with intelligence holdings and People's Liberation Army (PLA) operational requirements. PRC legal and institutional arrangements reduce barriers to that fusion. The 2015 PRC National Security Law broadly mobilizes citizens and organizations to support national security work and imposes duties of assistance and cooperation, while the 2021 Data Security Law creates categorized and graded data protection, defines "core national data," and directs the state to cultivate a data transaction market.[1] The U.S. Department of Justice (DOJ) Data Security Program rests explicitly on the premise that foreign adversaries will almost certainly employ commercially obtained U.S. data not only for surveillance and espionage, but also to support AI development and military capabilities.[2]

The operational implication is that data acquisition, access persistence, and disruption in time of crisis are no longer best understood as separate problems. They are components of a single operational continuum. The Office of the Director of National Intelligence (ODNI) assessed in 2025 that, if Beijing believed major conflict with Washington were imminent, it could consider aggressive cyber operations against military assets and U.S. critical infrastructure in order to

[1] "National Security Law of the People's Republic of China," DigiChina, translated by Rogier Creemers, Graham Webster, and others, July 1, 2015; "Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021)," DigiChina, translated by Graham Webster, Rogier Creemers, and others; Elsa B. Kania and Lorand Laskai, *Myths and Realities of China's Military-Civil Fusion Strategy* (Washington, DC: Center for a New American Security, January 28, 2021).

[2] U.S. Department of Justice, National Security Division, "Data Security," accessed April 21, 2026.

impede decision-making, induce societal chaos, and interfere with force mobilization.[3] The 2026 *Annual Threat Assessment* similarly warns that China retains the ability to pre-position for or conduct disruptive cyber operations against U.S. critical infrastructure, and specifically notes that U.S. intervention in a Taiwan conflict would probably bring "significant but recoverable disruptions to the transportation sector from Chinese cyber attacks."[4]

The Evolution of the Threat Posed by PRC State-Sponsored Cyber Actors

The scale of the threat posed by PRC state-sponsored cyber actors is exceptional. In January 2024, Federal Bureau of Investigation (FBI) Director Christopher Wray stated that "the PRC has a bigger hacking program than every other major nation combined" and that, even if every FBI cyber agent and intelligence analyst focused exclusively on China, "Chinese hackers would still outnumber FBI cyber personnel by at least fifty to one."[5] The precise ratio matters less than the structural reality it captures: Beijing can run parallel campaigns for espionage, target development, access brokering, transnational repression, and infrastructure pre-positioning with a depth of personnel and institutional redundancy that most defenders cannot match.

The target set also continues to widen. Chinese state-sponsored actors are not only targeting U.S. government and military networks and defense contractors; they are also targeting telecommunications providers, transportation systems, lodging, cloud and managed-service pathways, universities, local governments, and the civilian infrastructure on which mobilization depends. A multinational advisory issued in August 2025 warned that PRC actors were targeting telecommunications, government, transportation, lodging, and military-infrastructure networks globally.[6] Canadian authorities subsequently reported that likely Salt Typhoon actors had compromised Canadian telecommunications infrastructure in 2025.[7] And, U.S. authorities confirmed a broad and significant campaign against multiple major global telecommunications providers.[8]

---

[3] Office of the Director of National Intelligence, *2025 Annual Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, March 25, 2025), 12.

[4] Office of the Director of National Intelligence, *2026 Annual Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, March 18, 2026), 21.

[5] Christopher Wray, "Director Wray's Opening Statement to the House Select Committee on the Chinese Communist Party," Federal Bureau of Investigation, January 31, 2024.

[6] Cybersecurity and Infrastructure Security Agency, National Security Agency, Federal Bureau of Investigation, and partner agencies, "Countering Chinese State-Sponsored Actors' Compromise of Networks Worldwide to Feed Global Espionage System," Cybersecurity Advisory AA25-239A, August 27, 2025.

[7] Cyber Centre of the Canadian Centre for Cyber Security, "Cyber Threat Bulletin: People's Republic of China Cyber Actors Target Telecommunications Companies in Global Cyberespionage Campaign," June 2025.

[8] Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation, "Joint Statement from FBI and CISA on the People's Republic of China Targeting Commercial Telecommunications Infrastructure," November 13, 2024.

The sophistication of these operations is often misunderstood. Sophistication is not defined only by rare zero-days or bespoke implants. It is increasingly defined by the speed and scale of campaigning: "living off the land", exploiting known vulnerabilities at scale, abusing trust boundaries, hiding behind compromised routers or Internet of Things devices, and selecting infrastructure whose compromise yields strategic options.[9] The public record on Volt Typhoon, Salt Typhoon, and Flax Typhoon shows that PRC operators have become adept at turning ordinary weaknesses in edge devices, backbone infrastructure, and legacy administrative systems into durable access. This is not a lesser form of capability. It is evidence of mature campaign-level operations and a willingness to optimize for scale, deniability, and future utility rather than technical elegance for its own sake.[10]

These capabilities are enabled by systemic design, not just tactical tradecraft. The PRC uses a whole-of-government approach to technological power in which party-state priorities, industrial policy, intelligence work, and military modernization are mutually reinforcing. Military-Civil Fusion is central to this architecture. The Department of War (DoW) assesses that Beijing has elevated Military-Civil Fusion as a mechanism for channeling civilian technology, talent, and resources into military modernization and for moving military requirements back into the civilian sector, while recent academic work shows that nontraditional firms and research institutions are increasingly participating in the PLA's AI-related ecosystem.[11] The result is not just a tightly integrated military-industrial complex, but a broader system in which the state can draw on commercial research, logistics, talent, infrastructure, and data when it sees strategic advantage in doing so.

What does Beijing seek to gain from these operations? At minimum, four things: First, it seeks economic and technological advantage through theft or acquisition of intellectual property, operational know-how, and valuable datasets. Second, it seeks foreign intelligence and counterintelligence advantage at scale, especially the ability to identify, track, and profile high-value individuals and institutions. Third, it seeks operational preparation of the environment in U.S. and allied critical infrastructure and communications systems. Fourth, it seeks crisis leverage: options to slow mobilization, degrade decision-making, impose uncertainty, and raise the perceived cost of U.S. intervention in a Taiwan contingency or other confrontation.

---

[9] Federal Bureau of Investigation et al., "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," joint cybersecurity advisory, February 7, 2024; Federal Bureau of Investigation et al., "People's Republic of China-Linked Actors Compromise Routers and IoT Devices for Botnet Operations," joint cybersecurity advisory, September 18, 2024.

[10] National Cyber Security Centre, "UK and Allies Expose China-Based Technology Companies for Enabling Global Cyber Campaign Against Critical Networks," August 27, 2025.

[11] U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2025* (Washington, DC: U.S. Department of Defense, December 23, 2025), 54; Cole McFaul, Sam Bresnick, and Daniel Chou, *Pulling Back the Curtain on China's Military-Civil Fusion: How the PLA Mobilizes Civilian AI for Strategic Advantage* (Washington, DC: Center for Security and Emerging Technology, September 2025).

Why some PRC Actors Prioritize Persistence while Others Accept Attribution and Exposure

The distinction between PRC actors that persist quietly and those that accept attribution is best explained by mission objectives rather than by competence. In the persistence model, the objective is enduring access with high future value. Volt Typhoon's long-duration access to critical-infrastructure environments and Salt Typhoon's compromises of telecommunications providers fit this model. In such cases, the mission is not simply to steal a dataset and leave. It is to remain in the network long enough to understand architecture, dependencies, users, administrative rhythms, lawful-access interfaces, restoration pathways, and crisis utility.[12] The network itself becomes a strategic asset.

The underlying mission objectives of persistence campaigns are therefore threefold: strategic intelligence collection, target development, and option creation. A state-sponsored cyber actor that remains inside communications, energy, transportation, or water systems acquires not only information but also future leverage. This is why the repeated warnings about PRC pre-positioning matter so much. Their objective is not just to know more. It is to preserve their ability to act later, potentially during a crisis in which speed, uncertainty, and domestic disruption could shape the political context of U.S. decision-making.

Exposure-tolerant campaigns serve a different purpose. Their objective is speed, breadth, (sometimes) monetizable access, and broad target discovery rather than pristine secrecy. DOJ's 2025 cases involving i-Soon and actors linked to Advanced Persistent Threat 27 (APT27) show that some PRC-linked operators hacked at state direction and on their own initiative, then sold the resulting data or access to multiple Chinese state customers.[13] In these campaigns, attribution costs appear acceptable relative to the intelligence and commercial return. This is one reason U.S. analysis should not collapse all PRC cyber activity into a single bureaucratic model. The ecosystem includes formal intelligence services, contractors, access brokers, and data intermediaries operating with overlapping incentives.

It is therefore analytically useful to distinguish among the Ministry of State Security (MSS), the Ministry of Public Security (MPS), the PLA, and the contractor ecosystems that support them. MSS activity is often optimized for foreign intelligence collection and long-duration covert access. MPS activity more often overlaps with domestic control, transnational repression, and contractorized intrusion. PLA-linked or Military-Civil Fusion-enabled collection is particularly relevant to military modernization, logistics, and intelligentized warfare. Commercial firms, telecommunications providers, cloud vendors, and data brokers may serve as access pathways, collection surfaces, or integration points even when they are not formally part of the PLA. The United States should therefore think in terms of an ecosystem rather than a single monolithic actor.

---

[12] Federal Bureau of Investigation et al., "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure".

[13] U.S. Department of Justice, "Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns," March 5, 2025; U.S. Attorney's Office for the District of Columbia, "Chinese Nationals with Ties to the PRC Government and APT27 Charged in a Computer Hacking Campaign for Profit," March 5, 2025.

How PLA "Intelligentized Warfare" Could Weaponize the Data China Collects

The PLA's doctrinal evolution explains why data is so central to their way of war. Multi-Domain Precision Warfare (MDPW) is the PLA's core operational concept which leverages an integrated network of command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems to "identify and exploit weak points in the U.S. operational system," using AI to process and analyze enormous quantities of data. China views the next revolution in military affairs as a transition to this form of "intelligentized" warfare.[14] Scholarly work on PLA doctrinal development reaches a similar conclusion: data, machine-enabled analysis, and rapid decision support are not ancillary to future Chinese military operations; they are central to the PLA's concept of operational advantage.[15]

This doctrinal bridge connects peacetime data acquisition to wartime operational effect. The PRC is not collecting data simply for immediate intelligence value. It is collecting data to build a higher-resolution model of the U.S. operational system: who matters, where they are, what they depend on, where the bottlenecks are, and where limited disruption would create outsized effects. In U.S. military terms, this is the movement from espionage toward intelligence preparation of the environment.

Data on U.S. military personnel, cleared contractors, diplomats, intelligence personnel, and their networks is especially valuable because it collapses the boundary between physical and digital targeting. The Defense Intelligence Agency (DIA) has warned that "ubiquitous technical surveillance" (UTS) presents one of the most acute generalized threats to DoW and U.S. government personnel worldwide.[16] Geolocation, contact chains, travel patterns, device identifiers, health indicators, financial stress, and family or professional networks can be fused into targeting packages for surveillance, coercion, recruitment, and impersonation. This is not a hypothetical concern. Research on the U.S. data-broker ecosystem has shown that information on service members and veterans is commercially available in forms that would be useful to foreign intelligence services, and that the harms include profiling, influence targeting, coercion, and operational exposure.[17]

Data on weapons systems and the defense industrial base is equally important. Stolen engineering files, software baselines, testing data, and supplier relationships compress Chinese development cycles and reduce uncertainty in military modernization. At the operational level,

---

[14] U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2025*, 13.

[15] Elsa B. Kania, "Artificial Intelligence in China's Revolution in Military Affairs," *Journal of Strategic Studies* 44, no. 4 (2021); Yatsuzuka Masaaki, "PLA's Intelligentized Warfare: The Politics on China's Military Strategy," *Security & Strategy* 2 (2022).

[16] Lieutenant General Jeffrey Kruse, *2025 Worldwide Threat Assessment: Statement for the Record before the House Armed Services Committee* (Washington, DC: Defense Intelligence Agency, 2025), 36.

[17] Justin Sherman, Hayley Barton, Aden Klein, Brady Kruse, and Anushka Srinivasan, *Data Brokers and the Sale of Data on U.S. Military Personnel: Risks to Privacy, Safety, and National Security* (Durham, NC: Sanford School of Public Policy, Duke University, November 2023).

access to maintenance records, software dependencies, component sourcing, and contractor communications enables the construction of detailed target folders revealing sustainment vulnerabilities, patch cycles, single points of failure, and likely operational patterns. That information can support cyber effects, electromagnetic attack, deception, or kinetic targeting.

Logistics data may be even more consequential than platform data because modern military power projection is fundamentally a logistics problem. If China maps the civilian systems on which U.S. force projection depends—ports, rail chokepoints, fuel systems, airports, warehouses, medical networks, cloud logistics platforms, telecommunications carriers, and customs data—it can identify where limited disruption would create the most friction in deployment and sustainment. This is why PRC pre-positioning in critical infrastructure should be understood not only as a homeland-security issue but also as a force-projection issue. The most likely objective in a crisis is not generalized destruction. It is selective paralysis: enough friction to slow decisions and movement, divide policymaker attention, complicate escalation management, and raise the domestic cost of intervention.

Telecommunications data is central because it reveals who is communicating with whom, when, from where, and through which systems. Public statements by U.S. authorities on PRC targeting of commercial telecommunications have made clear that Chinese actors sought access to call-records data, selected communications, and other high-value information.[18] Commercial data flows into PLA intelligence and planning through several channels: direct cyber compromise of commercial entities, legal authorities that create state access pathways, contractor ecosystems that support intelligence services, and Military-Civil Fusion mechanisms that move commercial capabilities into military research and operations. A dataset does not need to be "military" at the moment of collection to become military in use.

There are also non-cyber collection pathways. The PRC can acquire strategically relevant data through data brokers, advertising technology and location-data markets, cloud and managed-service relationships, apps and platform ecosystems, research partnerships, healthcare and genomic collaborations, connected vehicles, Internet of Things deployments, logistics platforms, and ordinary commercial transactions. This is precisely why U.S. policy should not frame the problem solely as hacking. A strategically meaningful portion of the problem lies in how sensitive data is generated, aggregated, sold, licensed, and repurposed in ordinary commercial settings.

How China's Data Collection Fuels AI Advancement in the Commercial and Military Realms

China's data-acquisition strategy fuels AI in at least three ways. First, it provides training and fine-tuning inputs: source code, labeled data, domain-specific corpora, evaluation sets, and operational records that would otherwise be costly or time-consuming to obtain. The U.S.

[18] Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation, "Joint Statement from FBI and CISA on the People's Republic of China Targeting Commercial Telecommunications Infrastructure"; Cybersecurity and Infrastructure Security Agency et al., "Countering Chinese State-Sponsored Actors' Compromise of Networks Worldwide to Feed Global Espionage System".

Intelligence Community assesses that China seeks to become the world's most influential AI power by 2030 and accelerates that effort through both "licit and illicit" means, including cyber operations and intellectual-property acquisition.[19]

Second, China treats deployment itself as a data engine. A March 2026 paper for the U.S.-China Economic and Security Review Commission argues that China's open-source AI strategy and manufacturing dominance are mutually reinforcing, and that low-cost deployment of AI across factories, logistics networks, robotics, and other operational settings generates proprietary, real-world data that web scraping and synthetic generation cannot replicate.[20] This matters because the strategic value of stolen or purchased data is not limited to training frontier models. It also lies in accelerating applied AI in manufacturing, logistics, autonomy, and other domains with both economic and military value. This perspective is consistent with the growing scholarly literature on China's AI ecosystem, which increasingly emphasizes diffusion, operational iteration, and integration with the physical economy rather than benchmark performance alone.

Third, the same data can be routed into military AI. China is investing in AI for unmanned systems, intelligence, surveillance, and reconnaissance (ISR) collection and analysis, decision support, cyber operations, and information campaigns. Large language models (LLMs) and LLM-based reasoning models are useful for military tasks such as coding to assist cyber operations, question-answering to assist military decision-making, and synthetic-content generation to assist influence operations. The broader literature on Chinese military innovation reaches a similar conclusion: the PLA's interest in AI is not limited to autonomy in a narrow sense, but extends to decision support, cognitive operations, and the creation of information advantages across the battlespace.[21]

Biotechnology and health data deserve special emphasis because they sit at the intersection of data acquisition, AI, and national power. The U.S. Intelligence Community has reported that Beijing is investing heavily in collecting health and genetic data, regards genetic data as a strategic resource, and is expanding state control over gene banks and repositories.[22] In strategic terms, this is not merely a privacy issue. It is a dual-use industrial and national-security issue, with implications for biomanufacturing, precision medicine, force health, and future military applications of biotechnology.

The Most Urgent and Underappreciated Dimension of the Threat

The most urgent and underappreciated dimension of this challenge is the fusion problem: bulk

[19] Office of the Director of National Intelligence, *2025 Annual Threat Assessment*, 13.

[20] U.S.-China Economic and Security Review Commission, *Two Loops: How China's Open AI Strategy Reinforces Its Industrial Dominance* (Washington, DC: U.S.-China Economic and Security Review Commission, March 23, 2026).

[21] Elsa B. Kania, "Artificial Intelligence in China's Revolution in Military Affairs"; Josh Baughman, "The Path to China's Intelligentized Warfare: Converging on the Metaverse Battlefield," *Cyber Defense Review* 9, no. 3 (Fall 2024).

[22] Office of the Director of National Intelligence, *2025 Annual Threat Assessment*, 13; Elsa B. Kania, "Minds at War: China's Pursuit of Military Advantage through Cognitive Science and Biotechnology," *PRISM* 8, no. 3 (2020).

data acquisition, persistent access in telecommunications and critical infrastructure, and AI-enabled analysis are converging faster than U.S. policymakers can respond. Washington still tends to treat privacy, telecommunications security, critical-infrastructure resilience, AI competition, and defense mobilization as separate policy areas. Beijing does not. From Beijing's perspective, a dataset is valuable if it can reveal a vulnerability, identify a person, improve a model, shorten an innovation cycle, or shape a future battlespace. The strategic consequence is that the United States increasingly faces not isolated cyber incidents but the cumulative assembly of a decision-advantage architecture by a peer competitor.

The practical effect is a steady erosion of strategic sanctuary. Future conflicts will draw heavily on commercially generated data streams—including satellite imagery, civilian communications infrastructure, personal devices, and widespread sensor and video networks—as integral sources of intelligence and situational awareness. Recent Israeli operations against Iranian military and political leadership provide an illustrative example of what this can look like when intelligence preparation, cyber penetration, surveillance access, and data analytics are fused effectively. Public reporting suggests that Israeli operations in Iran drew on years of intelligence preparation, penetration of communications and internal systems, access to surveillance infrastructure and other digital data streams, and increasingly AI-assisted tools to identify patterns of movement and locate senior leaders with high precision.[23] The lesson for the U.S. government is clear: UTS is no longer a theoretical risk. It is already enabling the location, tracking, and targeting of senior government and military officials.

The economic dimension is underappreciated as well. This model taxes the United States twice: first through the direct cost of breaches, remediation, and disruption; second through the indirect transfer of research and development, operational tradecraft, and valuable real-world data into Chinese commercial and military systems. The challenge is not just theft. It is the conversion of U.S. openness into PRC state capacity. That is why the problem sits at the intersection of national security, industrial policy, privacy law, telecommunications security, and AI governance rather than neatly inside any one of those fields.

Recommendations

Because the problem is structural, Congress should respond holistically. The objective should not be limited to reducing the pool of strategically exploitable data or hardening the commercial systems that generate and transport it. It should also include changing the adversary's cost calculus, as articulated in the White House's 2026 cyber strategy.[24] For too long, Chinese cyber operations and data-acquisition campaigns have been rewarded by high returns and relatively manageable costs. An effective U.S. response must therefore combine denial, resilience, and cost

[23] Dake Kang and Sam Mednick, "Iran Built a Vast Camera Network to Control Dissent. Israel Turned It into a Targeting Tool," *Associated Press*, March 23, 2026; Greg Miller, "Israel Targets Iran's Leaders with Lethal Expertise Using New AI Platform," *Washington Post*, March 30, 2026; Doug Livermore, "By Fusing Intelligence and Special Operations, Israel's Strikes on Iran Are a Lesson in Strategic Surprise," Atlantic Council, June 15, 2025; Nilza Amaral, "The Iran War Highlights the Creeping Use of AI in Warfare," Chatham House, March 27, 2026.

[24] The White House, President Trump's Cyber Strategy for America (Washington, DC: The White House, March 6, 2026)

imposition: denying access where possible, hardening vulnerable systems where necessary, and imposing meaningful operational, legal, financial, and strategic costs on those who continue targeting the United States and its allies.

1. Impose sustained offensive pressure on PRC cyber operators and the infrastructure that enables them. Congress should support a standing campaign to disrupt, degrade, and hold at risk the infrastructure used by Chinese intelligence services, military elements, and contractor ecosystems to conduct cyber operations against the United States and its allies. This should include more persistent disruption of command-and-control infrastructure, botnets, access-broker networks, malware distribution channels, and contractor-operated intrusion platforms. The objective should not be episodic retaliation after major incidents. It should be to force PRC operators to spend more money rebuilding infrastructure, reconstituting access, protecting tradecraft, and defending against reciprocal pressure.

2. Force the PRC's cyber ecosystem onto the defensive by expanding authorities for active and continuous cyber campaigning. Congress should ensure that U.S. Cyber Command, the Intelligence Community, and relevant civilian agencies have the resources, legal authorities, and political backing necessary to conduct sustained campaigns that impose friction on Chinese cyber activity. That means more than just network defense. It means contesting Chinese cyber operators persistently enough that external intelligence collection becomes costlier and less predictable, and that Beijing must reallocate elite personnel and budget toward cyber defense, counterintelligence, and infrastructure recovery.

3. Target the contractor and commercial ecosystem that makes Chinese cyber operations scalable. The United States should not focus only on formal state organs such as the MSS, the MPS, or the PLA. It should also target the wider ecosystem of hacker-for-hire firms, data brokers, technology providers, telecommunications intermediaries, cloud-service entities, and other commercial actors that provide access, deniability, monetization channels, and surge capacity. Congress should support sanctions, procurement exclusions, civil and criminal actions, financial restrictions, export controls, and public exposure campaigns aimed at these firms. The goal should be to make participation in the PRC cyber ecosystem commercially dangerous and strategically costly.

4. Codify and expand a statutory national-security data control regime. The DOJ Data Security Program is an important start, but it still rests on executive emergency authorities. Congress should place the regime on durable statutory footing, preserve the transaction-based approach, and explicitly cover categories with obvious strategic value, including government-related data, precise geolocation, telecommunications metadata, genomic and health data, biometrics, financial data, advertising identifiers, connected-vehicle telemetry, and other linkable datasets whose combination produces targeting value.

5. Create a telecommunications and core-network security regime proportionate to the Salt Typhoon problem. Operators that carry significant communications traffic or store high-value metadata must be required to implement segmentation, logging, privileged-access controls, secure configuration baselines, rapid incident reporting, and independent testing and verification. The record now shows that telecommunications compromise is a national security issue, not

merely a private-sector cyber issue.

6. Pass a secure-by-design statute for internet-edge devices and network gear. The Volt Typhoon and Flax Typhoon cases show how PRC actors exploit routers, firewalls, network-attached storage devices, cameras, digital video recorders, and other long-tail devices to conceal identity, maintain access, and enlarge the attack surface. Minimum support periods, patchability requirements, secure defaults, end-of-life transparency, and procurement restrictions on unsupported equipment would materially reduce the infrastructure available for PRC concealment and persistence.

7. Establish special protections for military-adjacent commercial data. Precise location, device, financial, travel, health, and communications-related metadata associated with service members, cleared personnel, defense contractors, and sensitive military facilities should be presumptively restricted from foreign-adversary access whether the access comes through purchase, investment, vendor support, cloud administration, or cyber compromise. The logic of UTS makes clear that these data types are operationally sensitive, not merely privacy-sensitive.

8. Extend cyber and counterintelligence obligations beyond defense contractors to the wider operational ecosystem on which U.S. military power actually depends. In a Taiwan contingency, the most consequential targets may include ports, rail carriers, fuel distributors, telecommunications providers, hospitals, local governments near major installations, cloud providers, and logistics platforms that are not traditional defense primes but are nonetheless critical to force generation and sustainment.

Conclusion

In summary, China's cyber operations and broader data-acquisition strategy are best understood as part of a larger contest over information dominance, industrial capacity, and warfighting advantage. The PRC is collecting data not only to know more, but to act faster, shape markets, shorten innovation cycles, map vulnerabilities, identify people, and hold U.S. intervention infrastructure at risk. Military-Civil Fusion is the transmission belt. Cyber operations and commercial access are intake mechanisms. Artificial intelligence is the force multiplier. Intelligentized warfare is the operational concept that turns all of this into decision advantage. Congress should therefore treat this as a combined national-security data challenge: part cyber defense, part market regulation, part industrial policy, part counterintelligence, and part mobilization planning. If the United States continues to defend networks while leaving the underlying data economy strategically porous, Beijing will continue to convert commercial openness into military leverage.