April 30, 2026

Dr. Gregory Falco
Assistant Professor of Aerospace Engineering, Cornell University

Testimony before the U.S.-China Economic and Security Review Commission
Taking a Bigger Byte: China's Expanding Strategy for Data Dominance

Commissioners Leland Miller, Chris Slevin, and other esteemed members of the Commission, thank you for the opportunity to testify on China's expanding strategy for data acquisition and exploitation.

I design and test aerospace and defense systems for contested environments, with a focus on ensuring those systems remain secure and resilient to adversary exploitation. At Cornell University, where I direct the Aerospace ADVERSARY Lab, my work examines how adversaries use data, components, and system behavior to understand and gain advantage over complex technological systems.

I have led and supported research programs with organizations including DARPA, the U.S. Air Force Research Laboratory, the U.S. Space Force, and NASA, with a focus on space system security and autonomous systems. I have also contributed to U.S. congressional efforts on research security, including work supporting investigations into PRC-linked dual-use research infrastructure in the Arctic. In addition, I serve as Chair of IEEE's international standard on space system cybersecurity and as NATO Country Director for the HEIST program on hybrid space and subsea cable communications infrastructure.

The views expressed in this written testimony and during the hearing are my own and do not represent those of any institution with which I am affiliated. I also take individual responsibility for any unintended errors or omissions. I hope this testimony supports the Commission in developing actionable policy recommendations to address the growing risks associated with data-driven strategies and to strengthen U.S. technological leadership and security in an increasingly contested global environment.

To understand how the PRC data strategy works in practice, it is useful to look at how data is collected and used across different domains. Drones, scientific research infrastructure, space systems, and semiconductors may appear separate, but China approaches them in a consistent way. It extracts low-level data and turns it into pattern-of-life through aggregation and analysis at scale.

I will start at the tactical edge with drone systems and then expand outward to show how this same approach scales globally and across layers of technology.

Drones as a Data Collection and Inference Platform

In the drone ecosystem, the most valuable data is not the obvious data. It is not just imagery or high-end sensor payloads. The most strategically important data is low-level telemetry. Telemetry data is typically treated as benign, diagnostic, or operationally irrelevant. This

includes radio-frequency transmission patterns, GPS coordinates, inertial measurement unit (IMU) data, and subsystem-level power consumption. These are the exhaust signals of a system. Individually, they appear trivial. In aggregate, they are highly revealing.

The most important risk is that low-level telemetry data enables China to infer and anticipate U.S. testing activities and future operations, significantly reducing its reliance on traditional human intelligence collection methods. This represents a structural shift in intelligence collection. Historically, China would have needed human sources, access, or compromise to understand what the United States was developing or preparing to deploy. That model is increasingly obsolete. Today, that same insight can be derived passively from the routine operation of our own systems.

This works because telemetry is not random. It is structured, repeatable, and tightly coupled to system behavior. When multiple telemetry streams are correlated, they produce a behavioral signature of a mission. For example, elevated power draw combined with stable geolocation and minimal IMU variation can indicate persistent surveillance of a fixed site. In contrast, burst movement patterns, fluctuating power profiles, and dynamic navigation signals can indicate pursuit or tracking behavior in a tactical testing environment. These signatures are not hypothetical. They are observable, learnable, and scalable.

The real concern is not that any one drone reveals sensitive information. The concern is that large numbers of drones, operating across commercial and defense contexts, generate a continuous stream of structured data that can be aggregated and analyzed. In practice, this often takes the form of system logs and telemetry records that are routinely generated during operation and, in some cases, transmitted back to manufacturers or service providers.[i] China prioritizes scale in intelligence collection, gathering large volumes of data regardless of whether any single datapoint appears significant.

The historical constraint has been analysis. Human analysts cannot process telemetry at global scale. That constraint no longer exists. Advances in machine learning and inference systems now allow for the automated correlation of telemetry across massive datasets.

This has two immediate implications. First, it accelerates Chinese capability development. By observing how U.S. systems are operated, stressed, and tested, China can refine its own designs and operational concepts without needing direct access to the underlying technology. This is consistent with decades of industrial espionage, but now operates at a higher level of abstraction, focused on behavior rather than blueprints.

Second, and more strategically important, it enables anticipation. If China can observe testing patterns, system usage profiles, and mission signatures over time, it can begin to predict future operational activity. This includes identifying when a system is transitioning from testing to deployment, when new capabilities are being exercised, or when operational tempo is increasing in a way that suggests impending use. This is insight that was historically derived from classified sources. It is now increasingly available through open or compromised data streams.

Payload data reinforces and complements this capability. Electro-optical (imagery) and infrared sensors remain the most visible and widely discussed, but they are not the most interesting. Acoustic sensing, in particular, is underappreciated and highly revealing. Unlike imagery, which is constrained by line-of-sight and can be obscured by physical barriers, acoustic data can capture activity occurring inside facilities or behind structures. It provides access to processes, not just appearances.

Acoustic sensing can reveal the types of equipment in use and, importantly, the timing and progression of activity. For example, it can distinguish between idle systems and active processes, detect shifts in operational tempo, and identify repeated patterns of behavior.[ii] This is particularly valuable in environments where visual indicators are limited or intentionally concealed.

Outside of a propulsion test facility, acoustic data can be used to infer thrust regime or narrow the class of propellant by analyzing the combined frequency signature, temporal evolution, and amplitude profile of the emitted sound. Different propulsion systems generate distinct acoustic signatures as a function of combustion dynamics, exhaust flow, and structural interaction. These signatures are governed by physics and therefore repeatable. By tracking how these signatures evolve over time, an analyst can move beyond detection and determine how the test is being conducted, including its intensity, duration, and operational profile.

Importantly, the value of acoustic data is not in isolation. Its true power emerges when fused with other data streams. When combined with telemetry, geolocation, and RF sensing, acoustic signatures can be anchored in space and time, correlated with system behavior, and integrated into a broader inference framework. This type of acoustic inference becomes significantly more powerful when fused with telemetry, geolocation, and RF data, enabling high-confidence assessments of system behavior and operational intent.

This points to a broader issue. Drone systems should not be understood simply as platforms for sensing or actuation. They are continuous generators of data exhaust. That exhaust is structured, correlated, and increasingly accessible. When collected and analyzed at scale, it provides adversaries with a mechanism to understand what we are doing, how we are doing it, and what we are likely to do next.

The risk is not compromise. The risk is that normal system operation generates the data needed to understand and predict behavior. At scale, benign data becomes intelligence.

Scientific Research Stations as Dual-Use Data and Influence Platforms

While drone systems illustrate how low-level data can be aggregated to infer mission intent at the tactical edge, a similar dynamic is playing out at a much larger scale through global scientific research infrastructure. In this case, the focus is not on individual platforms, but on persistent sensing environments that enable continuous data collection across strategically important domains.

Scientific research stations are increasingly central to China's data acquisition strategy, not because of any single dataset, but because of how these platforms enable persistent, global, and strategically placed data collection under the guise of cooperation. The core idea is simple: environments that are scientifically valuable are also strategically valuable. China is investing in these locations to secure access, data, and long-term presence.

In areas where the United States has reduced its level of engagement in global scientific investment, openings are emerging that competitors are actively exploiting. China is deliberately filling the gap through a coordinated science diplomacy strategy, establishing strategically placed research stations that function as dual-use data collection platforms for both civilian collaboration and military-relevant intelligence gathering. This is not incidental. It is a deliberate positioning effort that prioritizes geographic advantage, data access, and long-term presence in regions that are otherwise under-resourced and under-observed.

One of the most important categories of data being collected through these platforms is ionospheric data. Remote and polar research stations are uniquely positioned to monitor the ionosphere, which can be treated as a large-scale, naturally occurring sensor. By measuring changes in radio signal propagation and localized disturbances in electron density, these systems can detect perturbations caused by high-energy events such as rocket launches or other space-based activities. These disturbances move through the ionosphere in measurable ways, allowing an external observer to detect and characterize events without direct observation.

The most important implication is that ionospheric sensing enables China to establish a passive, global early warning capability that can detect and characterize otherwise undisclosed U.S. space and launch activities without direct observation.[iii] This is a fundamentally different intelligence model. It does not require proximity, access, or intrusion. It relies on persistent sensing of the environment and the ability to interpret subtle physical effects at scale. In practice, this allows China to monitor testing activity, identify launch timing and location, and potentially distinguish between classes of events based on their disturbance profiles.

This space-domain sensing capability is paralleled by China's activities in the maritime and subsea environment, where scientific research platforms are used to collect seafloor mapping data and characterize undersea infrastructure. While these efforts are often framed as environmental or geological research, their strategic value lies in enabling precise mapping of subsea terrain and, critically, the location of subsea cable networks. These cables carry about 95 percent of global data traffic and are one of the most critical and vulnerable parts of the global information infrastructure.

The strategic risk is that precise mapping of subsea cables allows China to optimize the impact of targeted disruptions to global communications, either by severing critical links between countries or by forcing costly and time-consuming repairs that divert resources and attention. Recent increases in publicly reported subsea cable disruptions, often attributed to anchor drags, highlight the vulnerability of these systems. While some of these incidents may be accidental, the pattern is increasingly consistent with deliberate targeting behavior. This risk is further

underscored by the emergence of technologies such as specialized subsea cable cutting tools, which have limited commercial justification but clear operational relevance.[iv]

This risk is not hypothetical. Anticipating the strategic vulnerability of subsea infrastructure, we established the NATO Hybrid Space/Submarine Architecture to Ensure Information Security of Telecommunications (HEIST) program to develop resilience mechanisms for global communications, including the ability to reroute critical data flows through satellite networks in the event of cable disruption.[v] The need for such architectures reflects a growing recognition that subsea infrastructure is not only economically critical, but increasingly a targetable component of modern conflict.[vi]

Scientific research platforms are dual-use data collection systems. Activities framed as civilian science, such as atmospheric monitoring and seafloor mapping, directly support military targeting and operational planning. This is particularly evident in the Arctic, which has increasingly become a highly contested scientific environment, where data collection efforts align closely with infrastructure mapping and domain awareness objectives – both subsea and in space. The disruption of the Svalbard cable system, which supports satellite communications from polar orbits back to mainland networks, highlights both the importance and vulnerability of these assets. In this context, the line between scientific observation and operational preparation is increasingly blurred.[vii]

China's advantage in this domain is not just data collection. It is influence. Unlike traditional economic statecraft, this influence is not primarily about financial leverage. It is about trust. By positioning itself as a cooperative global actor through science diplomacy, China builds long-term partnerships in remote regions where few other actors are willing to invest. These are not purely financial transactional relationships. They are built on presence, continuity, and perceived alignment with local scientific and community needs.

This creates a powerful asymmetry. China becomes the default partner for research collaboration, gaining influence over who participates, what data is collected, and how that data is shared. In these environments, control over the sensing infrastructure translates directly into control over the data pipeline. This, in turn, enables control over the narrative derived from that data.

The result is not just data asymmetry, but narrative asymmetry. When a single actor controls both the collection and dissemination of scientific data, it can selectively release, delay, or curate datasets in ways that shape scientific understanding and geopolitical interpretation. A clear example of this dynamic can be seen in the China-Iceland Arctic Observatory. Chinese institutions have stated that ionospheric monitoring data from this facility is publicly available; however, in practice, this data is difficult to access or independently verify. This raises legitimate concerns about whether datasets are being selectively curated or modified prior to release, particularly when those datasets have strategic implications.[viii]

This is not a theoretical concern. It is an emerging operational reality. It is also the basis for initiatives such as the Secure Science Research Program, which is actively investigating research

sites globally where Chinese and Russian involvement may enable data control and potential manipulation. These efforts are aimed at understanding not just what data is being collected, but how that data is being governed, shared, and potentially leveraged for influence.

In this context, scientific research is no longer just a domain of collaboration and discovery. It is an instrument of strategic positioning. It enables persistent sensing, infrastructure mapping, and environmental monitoring, all of which have direct military relevance. At the same time, it builds trust, shapes partnerships, and influences how data is collected, shared, and interpreted globally.

Scientific research stations combine data collection, infrastructure mapping, and influence, making them one of the most effective and least scrutinized parts of China's data strategy.

Spacecraft as Targets for Capability Characterization and Counterspace Development

While terrestrial scientific research stations enable persistent sensing in remote regions of the Earth, space itself represents the next extension of this model. In many respects, spacecraft function as research platforms operating far beyond national boundaries, collecting data continuously across domains that are otherwise inaccessible. Like ground-based research stations, these systems are dual-use. They support civilian and commercial missions while also enabling military sensing and operations. As a result, space should be understood not just as an operational domain, but as a distributed, off-planet research infrastructure where data collection, experimentation, and strategic competition are increasingly intertwined.

In the space domain, China's objective is not simply to track U.S. spacecraft, but to understand what they are capable of and how they behave under stress. The most important data being sought is not positional data, which is widely available, but behavioral and operational data that enables capability characterization. This includes how spacecraft maneuver, how quickly they respond to external stimuli, and how their systems operate under different conditions.

China has demonstrated increasing sophistication in this area through on-orbit rendezvous and proximity operations (RPO). Systems such as the SJ-21 satellite, as well as experimental platforms like TJS-3, have exhibited the ability to maneuver in proximity to other spacecraft and conduct inspection-like activities. While these operations are often framed as servicing or experimental missions, they are inherently dual-use. The same capabilities required to approach and service a satellite are also required to observe, characterize, and potentially disrupt it.

The strategic value of these operations lies in what they reveal. By observing the frequency of maneuvers, the nature of orbital adjustments, and the responsiveness of a spacecraft to nearby activity, China can infer maneuverability and operational doctrine. These interactions are controlled probes. Rather than maintaining proximity, China conducts targeted, intermittent engagements to trigger a response. This is effectively a form of black-box testing in orbit.

By conducting intermittent proximity operations, China is able to improve its counterspace tactics by observing how U.S. space assets respond to controlled physical stimuli, revealing

readiness, response times, and operational redlines. This is not just about hardware. It is about behavior. China is actively seeking to map cause-and-effect relationships in the space environment: how quickly the United States detects an approach, how it responds, and what thresholds trigger action. This provides insight into escalation dynamics and operational boundaries in a domain where such information has historically been highly protected.

This capability directly supports the development of counterspace tactics, particularly in areas such as shadowing, close approach, and pre-positioning for potential disruption. Understanding how U.S. systems behave allows China to design operations that exploit timing gaps, avoid detection thresholds, or apply pressure without crossing perceived redlines. Proximity operations are not just demonstrations. They are data collection exercises used to inform future operations.

Parallel to these physical interactions, China is actively targeting the cyber layer of space systems. Cyber access to spacecraft provides a different but complementary form of insight. Rather than observing external behavior, cyber access allows an actor to understand internal system operation, including command structures, data flows, and mission execution.

China has shown interest in extracting sensitive information such as encryption keys from communications links, but the broader objective is to understand how U.S. space systems operate. Documented incidents, including previously reported intrusions involving Earth observation satellites such as Landsat-7 and Terra EOS, illustrate the potential for adversaries to gain access to spacecraft command and control pathways.[ix] Even limited access can provide valuable insight into how systems are configured, tasked, and managed.

This type of access enables capability characterization at a deeper level. It reveals how missions are executed, how systems respond to commands, and how resilient they are to interference. In parallel, China is probing the cyber layer of space systems, an area where my work on an international technical standard for space cybersecurity is focused.[x] These cyber operations are used to enable and enhance kinetic and operational effects, not replace them. Cyber operations in this context are not an alternative to physical counterspace actions; they are an enabler. They provide the information and access needed to make those actions more precise and effective.

An emerging and particularly concerning dimension of this effort is the application of adversarial machine learning to space systems. We have shown how autonomous spacecraft systems can be probed and degraded using carefully crafted inputs.[xi] This aligns with a growing body of Chinese technical work in this area. This convergence suggests increasing interest in understanding not just how spacecraft behave physically, but how their onboard decision-making systems operate.

Spacecraft autonomy is another surface for exploitation. By probing how a system responds to inputs, through proximity, RF, or cyber access, an adversary can infer how its onboard models operate. This enables a new class of counterspace tactics. Adversaries can manipulate the data a system relies on to drive incorrect behavior. In practice, this could involve feeding false or misleading inputs to degrade targeting, navigation, or situational awareness functions. This

extends the concept of “black-box probing” from hardware into the algorithmic layer, where the objective is not just to observe system behavior, but to actively shape it.

The integration of physical, cyber, and algorithmic data collection is further reinforced by trends in Chinese scientific research. A growing body of literature from Chinese institutions, including aerospace-focused universities and research laboratories, is focused on multi-agent spacecraft dynamics, cooperative maneuvering, and distributed space operations.[xii] While this research is academic in form, it aligns closely with the operational requirements of coordinated proximity operations and counterspace tactics. The volume and focus of this work suggest a sustained, systematic effort to translate observed behavior and collected data into operational capability.

China’s approach in space is consistent. It treats U.S. systems as observable and testable across physical, cyber, and algorithmic layers. It collects data through interaction and uses that data to develop counterspace capabilities. The objective is not just to match U.S. capabilities, but to understand them well enough to predict, counter, and potentially control their effectiveness in a conflict scenario.

Semiconductors as the Foundation for System-Level Data Extraction

Across drones, scientific research infrastructure, and spacecraft, the pattern is consistent. The most valuable insight comes from aggregating and interpreting low-level signals, not high-level data. Semiconductors sit at the foundation of this stack. Every system, from autonomous platforms to space assets, ultimately relies on chips that generate this data exhaust. China’s strategy does not stop at the system level. It extends down to the semiconductor layer, where the most granular and least protected data can be accessed and exploited at scale.

At the semiconductor level, China’s data acquisition strategy focuses on extracting insight from the lowest layers of system operation. The most valuable data is not high-level data. It is side-channel signals like power consumption and electromagnetic emissions that reveal how systems are operating in real time.

Side-channel data at the semiconductor level allows China to perform mission inference by extracting low-level signals such as power consumption and electromagnetic emissions, revealing what systems are doing, when they are operating, and how they are being used across platforms such as drones and satellites.

This capability mirrors the dynamics observed in higher-level systems: seemingly benign data, when collected and analyzed at scale, becomes highly revealing. At the chip level, power consumption patterns can indicate when systems are active, how intensively they are operating, and even the type of computation being performed, including cryptographic activity.

Beyond passive observation, China is also positioned to actively exploit semiconductor-level vulnerabilities. Techniques such as fault injection allow adversaries to bypass or weaken cryptographic protections. By bypassing encryption through fault injection, China is able to

access otherwise protected system data at scale, contributing to a broader data collection strategy aimed at learning how U.S. systems operate, behave, and can be exploited over time.

Taken together, semiconductors represent the foundational layer of China's data acquisition strategy. By extracting and exploiting low-level signals from chips embedded across critical systems, China can build a detailed understanding of system behavior that feeds directly into higher-level mission inference and capability characterization across domains.

Pattern-of-Life Data and Its Strategic Value

Pattern-of-life data is information that allows an observer to understand how a system is being used over time and to place that behavior in the context of its operating environment. It is not a single datapoint, but a collection of observations that, when aggregated, reveal purpose, intent, and function.

An intuitive way to understand this is through human behavior. If you observe when a person leaves their house, where they go, how long they stay, and how often they repeat that behavior, you can infer what they do for work, what they care about, and how they spend their time without ever directly asking them. The same principle applies to technical systems. By observing when a system operates, how it behaves, and how it interacts with its environment, an adversary can infer its purpose, priorities, and role within a broader mission.

This concept is already well established in large-scale sensing systems. Earlier in my career, I worked on urban sensing and data analytics, where similar techniques were used to understand behavior at the population level. China has applied these capabilities extensively to monitor and analyze population activity through continuous data collection.

The same approach is now being applied to machines. By collecting and aggregating low-level data from drones, spacecraft, and infrastructure, an adversary can build a pattern-of-life for those systems. This enables them to infer not just what a system is doing, but how it is being used and how it fits into a broader mission.

Pattern-of-life data becomes strategically powerful at scale because it allows an adversary to understand system capabilities and predict future behavior with high confidence. Over time, repeated observations transform isolated signals into structured knowledge. This enables anticipation, allowing an observer to predict what a system is likely to do next. This is especially possible today in the age of artificial intelligence, where advances in machine learning and large-scale data processing have removed the traditional bottleneck of human analysis. What was once too complex or voluminous to interpret can now be processed, correlated, and acted upon in near real time.

This concept is central to China's broader data acquisition strategy. China is not collecting data for isolated insights. It is building a large-scale data dragnet to extract pattern-of-life across systems and environments. The objective is to move from observation to prediction, and from prediction to strategic advantage.

The examples discussed earlier in this testimony illustrate how this operates across domains. In drone systems, low-level telemetry such as power consumption, RF transmission patterns, and navigation data can be aggregated to infer mission types and operational intent. In scientific research stations, persistent sensing of the ionosphere and subsea environment enables pattern-of-life detection of space launches and critical infrastructure usage, contributing to passive early warning and targeting capabilities. In the space domain, proximity operations and cyber access allow China to observe how U.S. spacecraft respond to stimuli, building an understanding of operational behavior and redlines over time. At the semiconductor level, side-channel signals such as power consumption provide a pattern-of-life for systems themselves, revealing when and how they are operating at the most granular level.

Across all of these domains, the underlying principle is the same: seemingly low-value, low-level data becomes highly strategic when collected, correlated, and analyzed at scale. Pattern-of-life is the mechanism that turns data into insight.

This is why pattern-of-life data is valuable in both commercial and military contexts. In commercial settings, it enables optimization by understanding user behavior and system usage. In military contexts, it enables anticipation and targeting by predicting behavior and identifying opportunities for disruption or exploitation. In both cases, the advantage lies in the ability to move from reactive to predictive decision-making.

Risks of Chinese Components in Critical Aerospace and Defense Systems

The primary concern with the proliferation of Chinese components in U.S. aerospace and defense systems is not limited to traditional notions of espionage, but rather the ability to perform large-scale pattern-of-life inference directly from within those systems. Embedded components provide a persistent and often overlooked source of low-level data that can be used to understand how systems operate over time.

Unlike traditional espionage, pattern-of-life data collected through embedded components can be passively, inconspicuously and continuously gathered at scale without human involvement as mundane log files, making it both low-risk to collect and difficult to detect because it appears as routine system data. This represents a fundamental shift from targeted intelligence operations to ambient data collection, where insight is derived from aggregation rather than intrusion.

When these components are present in aerospace and defense systems, the implications are particularly significant. Pattern-of-life inference from Chinese components embedded in these systems enables China to understand operational readiness, predict mission timing, observe system usage patterns, and infer capability deployment without direct access to the systems themselves. This allows an adversary to build a detailed operational picture based entirely on the routine functioning of U.S. assets.

This risk is not hypothetical. The technical capability to extract and analyze low-level system data is well established, and the growing body of research in Chinese technical literature reflects sustained interest in leveraging such data for system characterization and operational insight.

The concern is not that any single component is compromised in isolation, but that at scale, these components contribute to a broader data collection architecture that supports continuous monitoring and inference.

In this context, the proliferation of Chinese components should not be evaluated solely through a supply chain security lens, but as part of a larger data strategy. These components function as distributed sensing points within critical systems, enabling adversaries to collect the raw signals needed to build pattern-of-life at the system and mission level. The result is a form of persistent, low-visibility surveillance that is difficult to detect and even more difficult to counter once embedded.

Allied Responses and Constraints (NATO and Partner Nations)

U.S. allies, including NATO partners, are increasingly aware of the risks associated with foreign components in critical infrastructure and defense systems, but their responses remain uneven and, in many cases, constrained. The most significant challenge is the lack of a coordinated policy framework across allied nations, combined with differing perceptions of the threat. For some allies, the risks associated with embedded components and data collection are not yet viewed as urgent or are seen as comparable to concerns about reliance on U.S. technological dominance. This creates strategic ambiguity that slows unified action.

In addition, many allied nations operate under procurement regimes that emphasize non-discrimination and open competition, making it difficult to exclude specific foreign suppliers without clear, legally defensible justification. This legal structure can limit the ability to act preemptively, particularly in cases where risks are systemic and data-driven rather than tied to a specific, provable vulnerability.

Economic and political pressures further complicate the picture. Past cases in Norway, a close and highly valued NATO ally, such as the diplomatic and economic fallout following the awarding of the Nobel Peace Prize to a Chinese dissident, illustrate how China has used informal pressure to influence the behavior of smaller states. These dynamics are not unique to Norway and reflect broader challenges faced by open economies in a contested geopolitical environment. While not codified in formal agreements, such pressures can shape national risk tolerance and procurement decisions, particularly in countries that are economically exposed or sensitive to potential retaliation. In practice, this can lead to hesitation in restricting Chinese components, even when security concerns are recognized.

The result is a fragmented landscape in which some allies are moving aggressively to restrict high-risk components, while others continue to integrate them into critical systems due to cost, availability, or political considerations. This lack of alignment creates systemic risk across the alliance. Vulnerabilities in one nation's infrastructure can propagate across shared systems, supply chains, and operational networks, ultimately affecting collective defense capabilities.

This challenge is not just national. It is alliance-wide. Without greater coordination and a shared understanding of the risks associated with data-driven pattern-of-life inference, efforts to secure critical systems will remain uneven and incomplete.

Role of Standard-Setting Bodies in Securing Systems and their Data

Mitigating these risks requires embedding security directly into system design and development processes, making the role of standard-setting bodies central to protecting data across domains.

Standard-setting bodies play a critical role in securing data by defining the frameworks through which systems are designed, built, and integrated across international supply chains. Their most important function is to establish security requirements that enable interoperability while ensuring that security is not sacrificed for compatibility or cost.

The challenge with current standards is that they are either too prescriptive or too generic to be actionable. They also tend to add cost and overhead after systems are already built, rather than embedding security from the start. This creates a disconnect between compliance and actual security, particularly in mission-critical domains where speed and performance are prioritized.

The most important principle going forward is secure-by-design processes. This approach integrates security into system architecture and engineering decisions from the beginning, rather than applying it retroactively.[xiii] In practice, this means defining processes that guide secure decision-making without dictating specific technical implementations, allowing organizations to balance security, cost, and performance in a way that is appropriate for their mission.

International standards are particularly important in this context. They create a shared framework for trust across national boundaries and enable confidence and buy-in across a global supply chain. When security is built into the design process, it becomes something that can be consistently applied and verified across partners, rather than negotiated after the fact. This is critical for building a more trustworthy international technology ecosystem.

This approach is reflected in ongoing work within IEEE on space cybersecurity standards, specifically IEEE Std 3536-2026, where the focus is on establishing a process for secure system design rather than prescribing specific technical solutions. This effort has brought together more than 300 contributors from over 30 countries, reflecting the level of international coordination required to address these challenges. These frameworks draw on existing open-source guidance, such as SPARTA from The Aerospace Corporation, to provide visibility into known vulnerabilities and threat models.[xiv] By leveraging shared knowledge while allowing flexibility in technical implementation, such standards enable industry to make informed, economical design choices without compromising security.

Standard-setting bodies should therefore prioritize process-based, security-by-design frameworks that are adaptable, scalable, and aligned with real-world engineering constraints. In

doing so, they can play a central role in securing global systems while maintaining the interoperability and innovation that modern supply chains require.

Key Trends the Commission Should Track

While standard-setting bodies play a critical role in shaping how systems are designed and secured, it is equally important to understand how the broader technological and geopolitical landscape is evolving. The effectiveness of any standard ultimately depends on whether it keeps pace with emerging trends in how data is generated, collected, and exploited. Several developments are accelerating the strategic value of data and expanding the ways in which it can be leveraged by both the United States and its adversaries.

One of the most important trends the Commission should track is the rapid advancement of AI-enabled data fusion and inference. These capabilities are creating significant opportunities for efficiency and decision advantage across government and industry. However, the same technologies that enable the United States to better understand its own systems and operations also enable adversaries to perform similar large-scale inference on U.S. activities. This creates symmetry. The same capabilities that give us an advantage can be used against us. The removal of the human analysis bottleneck through artificial intelligence is fundamentally changing the scale and speed at which pattern-of-life can be constructed.

A second trend is the rapid expansion of dual-use infrastructure globally, particularly in environments where the United States has reduced its presence. China is exploiting this gap not through overt dominance, but by positioning itself as a cooperative and supportive partner in scientific and technical development. Through my work with NATO allies, I see this dynamic firsthand. It is especially evident in smaller but highly strategic countries where external engagement is welcomed and often necessary. China presents this as collaboration, but over time it builds persistent access to data, systems, and partnerships with clear strategic value. This model of engagement enables long-term influence without triggering the same level of scrutiny as more traditional forms of geopolitical competition.

A third trend is the growing exposure of sensitive data through globalized supply chains. As systems become more distributed and interconnected, data is increasingly generated, processed, and transmitted across components sourced from multiple countries. This creates a broad attack surface. Low-level data that is often assumed to be benign can be accessed and aggregated outside of U.S. control. The risk is not limited to any single component, but arises from the cumulative effect of widespread integration. Over time, this enables adversaries to build pattern-of-life across systems and operations without needing direct access to high-level data or networks.

Policy Recommendations

These issues are not isolated technical risks. They reflect a broader shift in how data is collected, interpreted, and used for strategic advantage. China's approach is systematic. It focuses on extracting insight from low-level data, building pattern-of-life across systems, and using that

understanding to guide both technology development and geopolitical positioning. Addressing this requires an equally systematic response that aligns policy, technology, and international engagement.

1. Strengthen Restrictions on Foreign Components While Enabling Trusted Alternatives

The United States should establish stricter requirements for the monitoring and restriction of foreign components in critical aerospace, defense, and infrastructure systems, with a particular focus on their potential to enable low-level data collection and pattern-of-life inference. Recent actions, such as provisions in the National Defense Authorization Act restricting the use of certain foreign-made drone components, represent an important and necessary step in addressing this risk. However, these measures have also highlighted the significant burden placed on research institutions and industry when alternatives are not readily available.

To be effective, restrictions must be paired with enabling infrastructure. This includes supporting the development of domestic and allied manufacturing ecosystems, ensuring the availability of trusted components, and aligning procurement practices with these objectives. Policymakers must also address cost realities, including whether the U.S. government is prepared to absorb higher costs for secure, trusted components in critical systems.

At the same time, secure-by-design approaches can provide a path to evaluate and, where appropriate, validate foreign suppliers. By requiring transparency in design processes and adherence to security-by-design frameworks, it becomes possible to assess risk based on how systems are built, not just where they originate. This creates a more flexible model, where trusted participation in the supply chain is earned through verifiable security practices rather than assumed based solely on country of origin.

Without these complementary measures, restrictions risk slowing innovation and mission delivery without fully mitigating underlying vulnerabilities.

2. Reinvest in Dual-Use Science and Global Presence

The United States should continue to strengthen its leadership in dual-use scientific and technical engagement, particularly in remote and strategically significant regions where data collection and infrastructure development are expanding. If the United States intends to double down on defense capability and high-TRL systems for the warfighter, it must also double down on scientific presence and influence in the environments where the underlying data and infrastructure are being established.

Recent shifts away from international scientific engagement, even if driven by a focus on domestic capability and defense priorities, carry strategic risk if not balanced with outward-facing presence. In practice, reduced engagement creates openings that competitors are actively exploiting. China is positioning itself as a cooperative and supportive partner in these regions, establishing long-term access to research environments and data-generating infrastructure under the banner of collaboration.

This has direct strategic consequences. Control over scientific research sites, especially those with dual-use capabilities, means control over data collection and access. Over time, it also means control over how that data is interpreted. This creates both technical advantage and influence over how key domains are understood and governed.

Congress should prioritize sustained investment in international scientific partnerships that align with U.S. strategic interests, particularly in regions where scientific infrastructure is being built and expanded. This does not conflict with an America-first approach. It reinforces it. Maintaining leadership requires being present where data is generated and where future systems are being shaped.

This includes expanding collaboration with allies in areas with clear defense and dual-use relevance. Programs such as Fulbright, administered by the Department of State, should be expanded to support security-focused research tracks and placements in strategically important regions. These efforts should be coordinated with agencies such as the Department of Defense, the National Science Foundation, and the Department of Energy to ensure alignment with national security priorities and emerging technology areas.

Congress should also support the creation of joint research and testing initiatives with allied nations, including shared facilities and field environments where technologies can be developed and evaluated in operationally relevant conditions. These collaborations should focus on building real capability, not just exchanging information, and should strengthen long-term partnerships in regions where data access and infrastructure are increasingly contested.

At the same time, the United States should prioritize and incentivize scientific work with dual-use relevance, particularly at higher technology readiness levels where research can transition into operational capability. This directly supports current efforts to accelerate defense innovation and deliver capability to the warfighter. Policymakers should encourage researchers to engage with the defense ecosystem and ensure there are clear pathways to translate research into deployable systems. This includes expanding funding mechanisms, fellowships, and incentives that make it easier for researchers to work at the interface of science and national security.

You cannot secure what you do not see, and you cannot see what you are not present to observe.

3. Promote Security-by-Design Through Standards and Procurement

Congress should support the development and adoption of security-by-design standards across critical systems, including the adoption of internationally aligned frameworks. These standards should emphasize process-based approaches that integrate security into system architecture from the outset. Current standards are either too prescriptive or too generic, and they lack objective technical criteria. They also add cost after the fact instead of building security in from the start. This approach is insufficient for addressing the evolving risks associated with data-driven system exploitation.

Instead, standards should define processes that guide secure decision-making without mandating specific technical implementations. This enables organizations to balance security, cost, and performance while still adhering to robust security principles. When aligned internationally, these frameworks also create a shared basis for trust across partners and suppliers, enabling more secure and interoperable global supply chains.

Work within IEEE, including IEEE Std 3536-2026 on space cybersecurity, reflects this approach by establishing structured processes for secure system design while drawing on open-source resources such as SPARTA to inform risk awareness. These efforts demonstrate how security-by-design can be applied consistently across organizations and countries, while still allowing flexibility in implementation.

By promoting flexible, process-based standards and aligning procurement requirements with these principles, Congress can help ensure that security is embedded into systems from the beginning, rather than retrofitted after vulnerabilities emerge.

Conclusion

These recommendations address the core challenge outlined in this testimony. Low-level data is becoming strategically valuable, and when aggregated at scale, it can be turned into actionable insight. China's approach is consistent. It focuses on extracting pattern-of-life across systems and environments.

To respond effectively, the United States needs to move beyond reactive measures. It must secure the foundational layers of its systems, maintain a presence in key data-generating environments, and embed security into system design and governance from the start.

This competition is about understanding how systems operate and turning that technical understanding into strategic advantage.

---

[i] Mozur, P. (2017, November 29). Drone maker D.J.I. may be sending data to China, U.S. officials say. The New York Times. https://www.nytimes.com/2017/11/29/technology/dji-china-data-drones.html

[ii] Terwilliger, A. M., & Siegel, J. E. (2022). Improving misfire fault diagnosis with cascading architectures via acoustic vehicle characterization. Sensors, 22(20), 7736. https://doi.org/10.3390/s22207736

[iii] Boschetti, N., Nikas, I., Sharma, S., & Falco, G. (2024, March). A global ionosphere situational awareness architecture for over the horizon radar operations. In *2024 IEEE Aerospace Conference* (pp. 1-9). IEEE.

[iv] Tatlow, D. K. (2025, January 10). Exclusive-Chinese patents reveal aim to cut undersea cables. Newsweek.

[v] Boschetti, N., Koyyada, A., Downs, B., Rosenthal, W., Gordon, N., Liwång, H., ... & Falco, G. (2025). Hybrid Space and Submarine Architecture to Ensure Information Security of Telecommunications (HEIST). *IEEE Access*, *13*, 193765-193785.

[vi] Potter, N. (2025, January 30). *NATO's emergency plan for an orbital backup internet*. IEEE Spectrum. https://spectrum.ieee.org/undersea-internet-cables-nato

[vii] Boschetti, N., Sigholm, J., Wallen, M., & Falco, G. (2023). A hybrid space architecture for robust and resilient satellite services. In 2023 IEEE 9th International Conference on Space Mission Challenges for Information Technology (SMC-IT) (pp. 114-122). IEEE. https://doi.org/10.1109/SMC-IT56444.2023.00021

[viii] Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party. (2024, October 16). PRC dual-use research in the Arctic [Letter]. U.S. House of Representatives.

[ix] U.S. House of Representatives, Committee on Oversight and Government Reform. (2012). *Cybersecurity: Assessing the immediate threat to the United States* (112th Cong., CHRG-112hhrg72919). U.S. Government Printing Office. https://www.congress.gov/112/chrg/CHRG-112hhrg72919/CHRG-112hhrg72919.pdf

[x] Falco, G., Henry, W., Aliberti, M., Bailey, B., Bailly, M., Bonnart, S., ... & Wallen, M. (2022). An international technical standard for commercial space system cybersecurity-a call to action. In *ASCEND 2022* (p. 4302).

[xi] Thummala, R., Sharma, S., Calabrese, M., & Falco, G. (2024). Adversarial machine learning threats to spacecraft. *arXiv preprint arXiv:2405.08834*.

[xii] Tang, X., Ye, D., Low, K. S., Luo, S., & Sun, Z. (2023, March). Multi-spacecraft pursuit-evasion-defense strategy based on game theory for on-orbit spacecraft servicing. In 2023 IEEE Aerospace Conference (pp. 1-9). IEEE.

[xiii] Viswanathan, A., Bailey, B., Tan, K., & Falco, G. (2024, May). Secure-by-component: A system-of-systems design paradigm for securing space missions. In *2024 Security for Space Systems (3S)* (pp. 1-9). IEEE.

[xiv] The Aerospace Corporation. (n.d.). *SPARTA (Space Attack Research and Tactics Analysis) framework*. https://sparta.aerospace.org