The Red Flag 14-1 cyber protection team works on defense procedures inside the Combined Air and Space Operations Center-Nellis during the exercise February 5, 2014, at Nellis Air Force Base, Nevada. The CPT's primary goal is to find and thwart potential space, cyberspace, and missile threats against U.S. and allied forces. (U.S. Air Force photo/Senior Airman Brett Clashman)

Cyberspace Collaborative Awareness

A Model for Unity of Effort in Homeland Defense

By Michael Knapp, Sean Atkins, and Matthew McLaughlin

A renewed wave of cyberattacks on critical infrastructure calls into question the United States' ability to combat cyberspace threats to the systems the nation relies on most. Chinese, Russian, and Iranian intrusions into the systems underpinning American society—such as utilities, communications, and transportation—dramatically increased in scope and scale from 2022 to 2024, to nearly 13 attacks per second worldwide.[1] During the same period, known cyberattacks on infrastructure increased by 30 percent.[2] As one Department of Homeland Security (DHS) official explained, "[Malign cyber actors] have the access that they need, and if the order was given, they could disrupt some services in this country right now."[3]

The fact that U.S. critical infrastructure systems remain at demonstrably greater risk despite massive national investment in cyber defense indicates that some underlying fundamentals

Lieutenant Colonel Michael Knapp, USAF, is the Deputy Director for Congressional and Interagency Affairs at U.S. Transportation Command. Lieutenant Colonel Sean Atkins, USAF, PhD, is the Commander of the 21st Student Squadron at the USAF Air Command and Staff College. Commander Matthew McLaughlin, USN, is the Reserve Fleet Forces Liaison Officer to U.S. Northern Command.

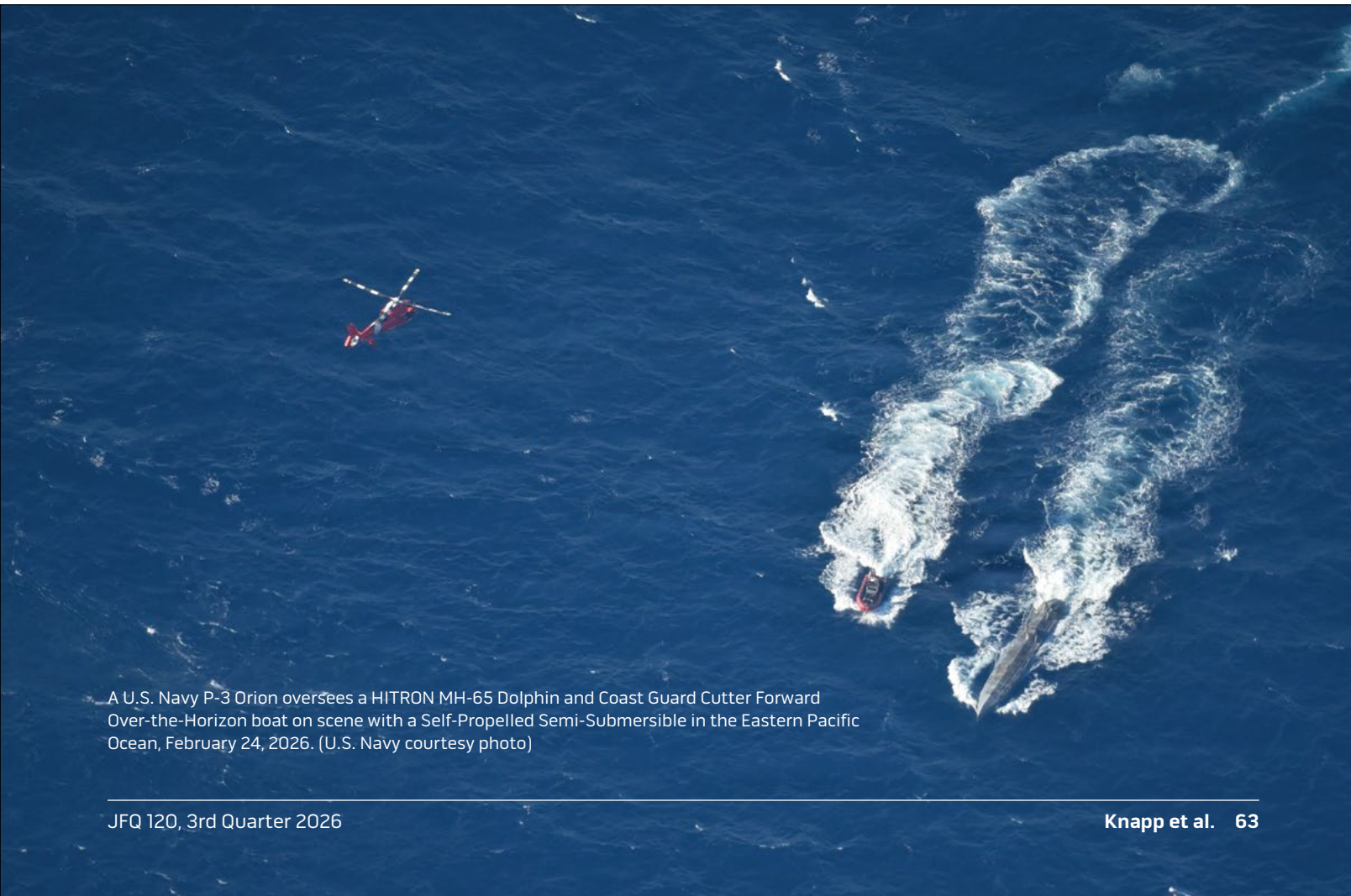
may be wrong.[4] Senior joint force commanders and members of Congress increasingly highlight the importance of one such fundamental—cyber domain awareness. This is a particularly critical issue for U.S. Northern Command (USNORTHCOM), the organization vested with the responsibility and authorities to defend the homeland across all domains. Indeed, during the closing months of his command of USNORTHCOM, General Glen D. VanHerck testified to Congress that a lack of awareness in the cyber domain hobbled homeland defense efforts:

As competitors and potential adversaries continue to field advanced all-domain capabilities with the potential to create significant effects in the homeland, it is imperative that the United States and Canada move quickly to improve domain awareness from the seafloor to space and cyberspace for all approaches to North America. [Improved awareness capability] will directly correlate to more time available to leaders at all levels, enabling the creation and employment of better deterrence options and, if required, defeat options.[5]

The complexity of roles and responsibilities in cyberspace is a nontrivial issue, as private industry owns and operates most of the nation's critical infrastructure, making private firms essential homeland defense and security players. Such ambiguity presents inherent difficulty coordinating between Federal agencies and American industry, thereby hindering unity of effort for homeland defense. In the absence of unity of command across disparate infrastructure cyber systems and actors, homeland defense requires a unity of effort based on a basic shared domain awareness.

Though efforts at developing shared awareness of cyber threats and risks have existed since at least the 1990s,[6] it was only in 2019 that Congress authorized the U.S. Cyberspace Solarium Commission to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyberattacks of significant consequences."[7] The commission emphasized that establishing an "enhanced level of situational awareness" was critical to countering cyberattacks.[8] In 2024, Congress considered legislation directing DHS to deepen collaboration among Federal agencies, industry, and partner nations to defend against and recover from cyberattacks.[9] As the conversation around cyber defense continues to mature, national leaders and practitioners should contemplate how lessons from other domains can inform characteristics of cyber domain awareness.

Government-civilian partnerships in other domains provide successful examples of unity of effort for homeland defense. For instance, the Department of War (DOW) and Department of Transportation maintain awareness of American airspace; an interagency consortium primarily led by the U.S. Coast Guard and U.S. Navy monitors American waters; and DOW, the National Aeronautics and Space Administration



A U.S. Navy P-3 Orion oversees a HITRON MH-65 Dolphin and Coast Guard Cutter Forward Over-the-Horizon boat on scene with a Self-Propelled Semi-Submersible in the Eastern Pacific Ocean, February 24, 2026. (U.S. Navy courtesy photo)

(NASA), the Department of Commerce, and various private operators share responsibility for space domain awareness. However, despite the myriad individual efforts within pockets of industry and government, current arrangements for the cyber domain may not effectively counter the coordinated cyber campaigns facing the United States. At the most basic level, there is no agreed-upon cyber domain awareness concept to guide unity of homeland defense efforts.

An examination of public-private partnerships in the air, maritime, and space domains reveals general domain awareness features that enable government, joint force, and industry leaders to gain "a common understanding of the situation" and synchronize defense efforts.[10] For the cyber domain, a *collaborative awareness* construct based on three foundational principles—visibility, sensemaking, and shareability—contributes to unity of effort in homeland defense.

The Building Blocks of Awareness

On the most basic level, awareness begins with the individual player in an environment. Individuals can broaden their comprehension of the system by aggregating their awareness with others' understanding to create team awareness or the "active construction of a model of a situation partly shared and partly distributed between two or more agents, from which one can anticipate important future states."[11] Combinations of teams and individuals can build collaborative situational awareness, in which no single entity maintains a common operating picture; instead, relatively seamless sharing permits different players to have the information they need for their respective missions.

Situational awareness, the conceptual cornerstone of collaborative awareness, has been studied in military flight operations since World War I.[12] Later, in the 1980s, human factors researchers extended their situational awareness studies to civil aviation and the air domain writ large.[13] The most widely accepted definition of *situational awareness* is a three-level perception, comprehension, and projection model, illustrated in figure 1.[14] The model identifies the first level of situational awareness as mere perception of the environmental cues. The second level understands Level 1 data within the context of current tasks. Finally, the third level combines Levels 1 and 2 data to project future system states.[15]

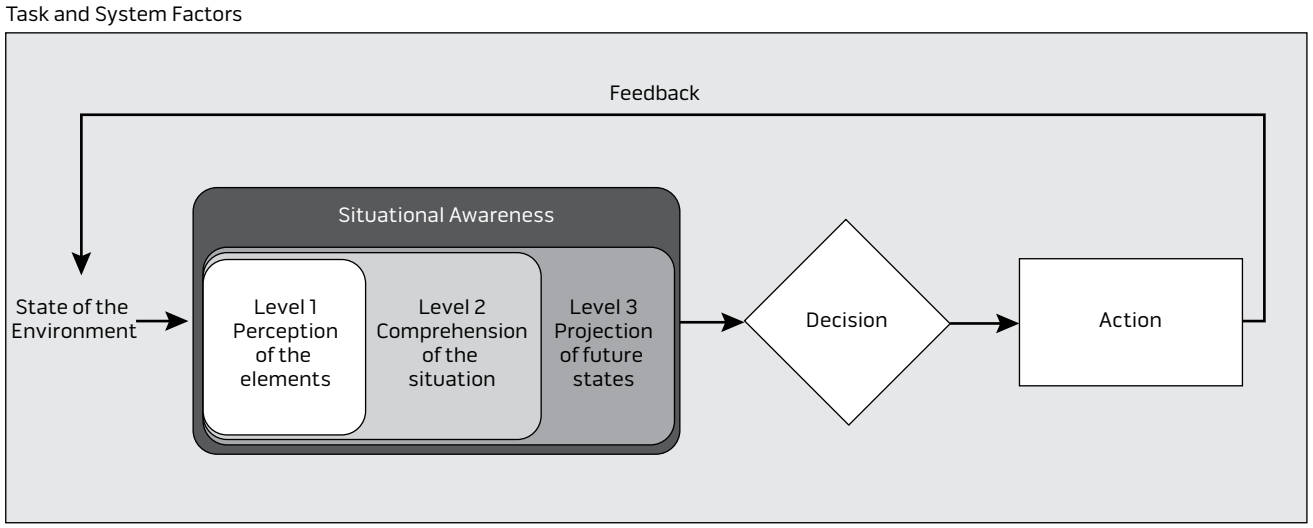
While this model of situational awareness is helpful, it fails to consider the shared awareness of multiple team members. The concept of *team awareness* considers the interactions of multiple team members or players seeking to understand the environment. This model overlaps individual players' zones of situational awareness and considers the now-shared situational awareness elements. Layered awareness allows the individual players to better perceive, comprehend, and project situational awareness in their and others' roles. Figure 2 depicts where the awareness of individual players is exclusive and where it is shared.

Furthermore, a shared mental model allows team members to track other players' activity without linear communication processes. Shared mental models "provide team members with a common understanding of who is responsible for what task and what the information requirements are. In turn, this allows individual players to anticipate one another's needs so that they can work in sync."[16] The shared mental model derived from team awareness undergirds the unity of *any* effort, let alone national security efforts.

Essentials of Collaborative Awareness

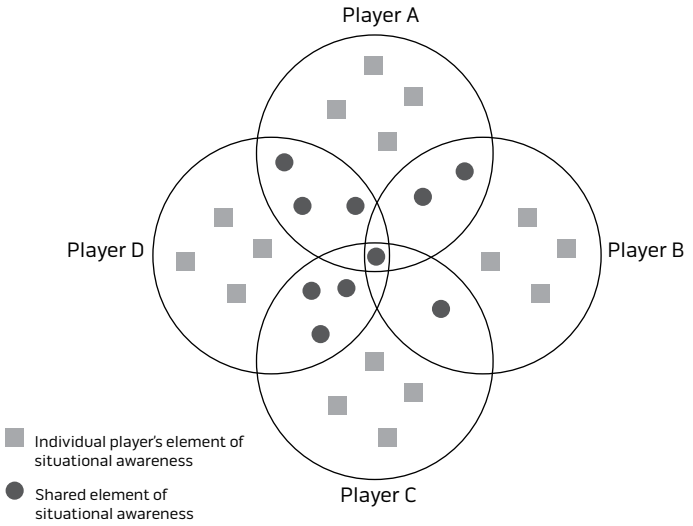
The complexity of the cyber domain and the overlapping equities of its many stakeholders in and out of government muddles earnest attempts at coordinating actions in cyberspace. Rather than building a massive

Figure 1.



Source: Authors.

Figure 2.



Source: Authors.

common operating picture of the cyber environment, national security leaders should endeavor to construct *collaborative awareness*, enabling mutual support among the many players in U.S. cyberspace.

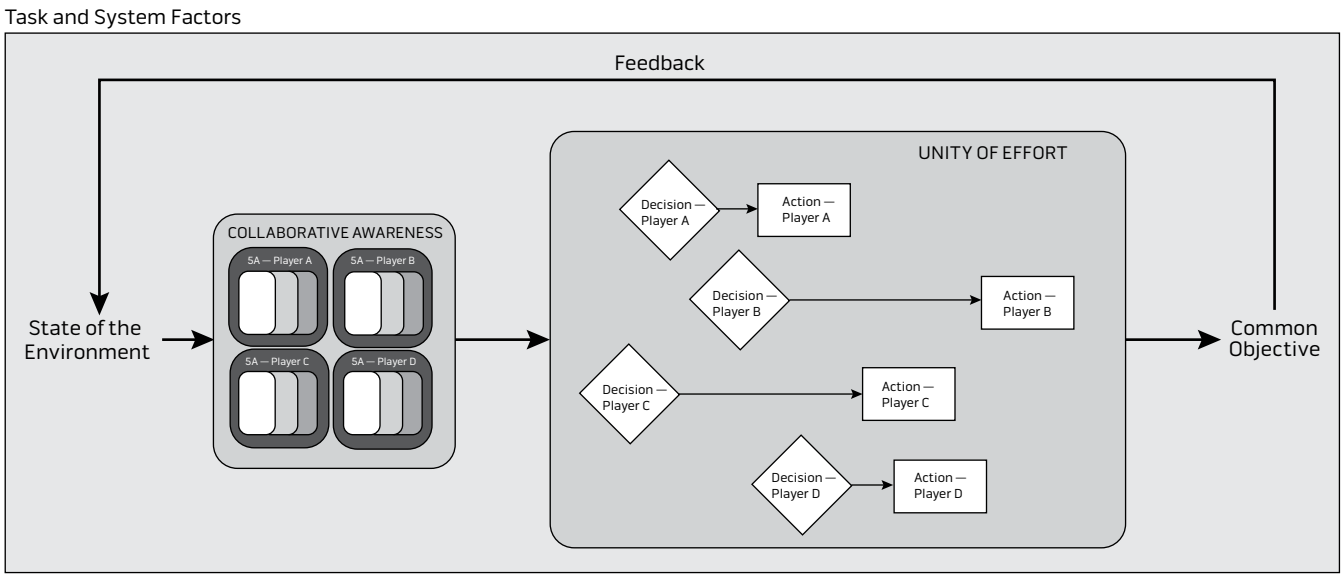
Collaborative Awareness Defined

While human factors researchers assumed that players in a team awareness model would likely have access to the same information, a collaborative awareness framework does not include this assumption. It acknowledges cognitive limits and the role of mission imperatives by providing enough information for making independent decisions toward a common goal but not enough for a complete common operating picture. Figure 3 illustrates a proposed model of collaborative awareness for the cyber domain.

In the collaborative awareness model, tasks, systems, and other factors interact within the environment, impacting the shared awareness of individual players. For the cyber domain environment, external factors like electromagnetic spectrum dynamics, internal factors like changing network architectures, and even ambient factors like hurricanes and their impact on infrastructure all affect the environment. Individual players ingest these factors to shape their situational awareness, and the players communicate their separate instances of situational awareness with others to enhance team awareness. Then, the system builds collaborative awareness in which no player has complete awareness, but all players have enough to make decisions. This shared understanding allows players to make decisions and undertake actions on independent timelines toward a common objective, producing unity of effort. Continuously, feedback loops shape the environment and update the players' shared collaborative awareness.

Collaborative awareness allows for the variability and organizational caveats inherent to the cyber domain. Private firms primarily own the hardware and software that form the basis of the cyber domain and may need to protect certain proprietary information as they protect their networks. Government agencies enact

Figure 3.



Source: Authors.

public policy but also may need to protect classified sources or methods. Collaborative awareness and deliberate, measured information-sharing permit players to take required action—including offensive actions for which DOW is authorized—without exposing sensitive information.

Analysis of other domains shows potential foundational principles of collaborative awareness in visibility, sense-making, and shareability. Applying these three principles will help cyber players achieve collaborative awareness on the meta-system level.

Visibility: Ability to Observe Domain Activity

The first principle required for effective collaborative awareness—visibility—describes a player's ability to monitor activity throughout the domain. From the team awareness model, certain players in the environment may perceive only some activity elements. In that case, any player's visibility must also extend to assimilating elements that only other players perceive. Importantly, visibility involves perceiving both the presence and absence of expected cues, which presents its own challenges. Existing awareness models in the air, maritime, and space domains provide examples of the visibility principle.

Visibility for air domain awareness incorporates a range of environmental cues to support flight safety for civilian aircraft and threat tracking for military applications. Whether air traffic control is provided by a Federal agency in the United States or a private nonprofit in Canada, the flight control body must comprehend internal and external factors to build awareness of the domain. For instance, to best picture the air domain, controllers must understand an aircraft's physical particulars like speed or altitude, airport conditions like runway closures or taxiway issues, and ambient factors like thunderstorms or outages of global satellite navigation systems. Merely possessing the ability to perceive these environmental factors is not sufficient—interagency processes must also exist to facilitate information sharing and amplify collaborative awareness.

The aircraft hijackings of September 11, 2001, demonstrated two visibility failures. First, air traffic controllers lost track of American Airlines Flight 77 over Ohio after terrorists maneuvered the plane unexpectedly. Initially, radar

U.S. Marines operate an Autonomous Low-Profile Vessel at Naha Military Port, Okinawa, Japan, January 17, 2025. Marines with 12th Littoral Logistics Battalion executed the first ALPV rehearsals in Okinawa, increasing 12th LLB's operational readiness and amphibious capabilities. The ALPV is a semi-submersible autonomous logistics delivery system that has the ability to deliver multiple variations of supplies and equipment through contested maritime terrain. The Marines are with 12th LLB, 12th Marine Littoral Regiment, 3d Marine Division. (U.S. Marine Corps photo by Lance Cpl. Rodney Frye) (Details on the vessel have been blurred for security reasons)

software configurations prevented controllers from seeing the aircraft for 8 minutes. Once radar coverage was technically reestablished, controllers scanned the wrong geographic area, not noticing the plane had turned to the east earlier.[17] In this instance, both technical and procedural issues negatively impacted visibility within the environment. Second, the Federal Aviation Administration (FAA) and North American Aerospace Defense Command (NORAD) failed to build effective team awareness by communicating updated situational awareness factors. On the morning of September 11, NORAD launched multiple fighter aircraft to intercept the hijacked commercial planes. One fighter formation initially flew out over the Atlantic and not toward Washington, DC, ignorant of the FAA's radar tracks. NORAD scrambled other fighters from the Midwest on a false intercept, even while the nearby United Airlines Flight 93 crashed outside Shanksville, Pennsylvania.[18] In both cases, the FAA and NORAD maintained separate awareness of the domain as radar systems were not integrated, and independent visibility of environmental factors was not shared.

Visibility in the maritime domain is typified by information shared globally among players to establish rudimentary domain awareness via basic factors like data on ship positions and crew and cargo manifests. Other environmental factors, such as weather patterns and the bathymetric characteristics of the ocean (for example, tides and depth), are essential to safe navigation and contribute to overall awareness of the domain.

However, drug-smuggling submersibles highlight a visibility weakness at the edges of current maritime domain awareness. These submersibles and semisubmersibles generally travel at low speeds and present minimal silhouettes above the waterline, if any. Since 2006, narco-cartels have continually innovated the vessels' design to avoid detection, which appears to be working. Though numbers are murky, Colombian cartels produced an estimated 2,664 metric tons of cocaine in 2023, while the U.S. Coast Guard interdicted only 96 metric tons of cocaine in the Caribbean that same year.[19] The dynamism of the environment and evolution of adversaries' technology requires expanded partnerships "with 15 different interagency partners . . . and . . . 20 different countries" to overcome this maritime domain awareness gap.[20]

Space illuminates unique aspects of visibility for collaborative awareness. For one, space domain awareness incorporates observable factors and the absence of anticipated observations or *deviations from the expected*. Additionally, players depend on techniques and technology in other domains to build situational awareness in space.

In the space domain, U.S. Space Command and the U.S. Space Force track all orbital objects, whether military or commercial, U.S. or foreign, or natural or artificial. Space provides no cover or concealment, and orbital motion is Newtonian; therefore, all objects are theoretically observable to ground stations, and their future positions can be predicted with high fidelity. Any deviation from an object's expected path alerts authorities to possible system anomalies, benign or malicious. While primarily intended for traffic management and collision avoidance in an ever-more congested environment, this awareness based on path anomalies may also clue players into malign activities in a domain that is ever more contested.

Because of limited access to space, operators must integrate quickly evolving technologies to build awareness. For instance, current sensor capabilities may not detect maneuver dynamics from emerging orbital technologies such as ion thrusters or solar sails, or satellite tracking capabilities may be outpaced by dramatically growing constellation sizes. Meeting these dynamic visibility needs requires space operators, including DOW, to adopt new sensing technology at a rapid rate. And looking holistically, space awareness also depends on awareness in other domains. A satellite launch, for example, requires maritime domain awareness to maintain clear areas downrange of the launch site, air domain awareness for aircraft deconfliction and weather, and space domain awareness for nearby orbital traffic and solar activity.

The previously examined domains demonstrated the importance of integrating multiple public and private players to build collaborative awareness. Failures on September 11, challenges in undersea observation, and growing commercial satellite constellations each offer lessons related to the visibility principle. Intentionally designing visibility could promote collaborative awareness in cyberspace and support homeland defense efforts.

Sensemaking: Characterization and Projection

The second principle underlying collaborative awareness—sensemaking—builds upon the second and third levels of the situational awareness model. First, a player parses visible and shared factors in the environment to comprehend their position. Then, the player combines their situational awareness with that of others to project future behaviors. While the factors within the environment may differ from domain to domain, making sense of the environment, or characterizing it, and then projecting actions is fundamental to collaborative awareness.

Characterization, the first dimension of sensemaking, involves understanding internal, external, and ambient factors affecting new objects of interest in the environment. In the maritime environment, for example, U.S. Navy ships observe radar returns or positioning data to classify neighboring vessels. Comparing these internal and external factors to known traffic patterns, military operators can then characterize objects in the environment as friendly, neutral, or hostile. And, as much as a vessel's physical characteristics may matter, understanding external and ambient factors like a ship's ownership and registration scheme expands the understanding of the domain. For instance, an obfuscated ownership scheme may indicate that a vessel participates in illicit activity. In one example, opaque registration and neglected position reporting (that is, a deviation from the expected) have permitted North Korea to conduct at-sea transfers of oil with

A U.S. Marine Corps F-35B Lightning II assigned to Marine Fighter Attack Squadron (VMFA) 121, 31st Marine Expeditionary Unit, prepares to take off during flight operations in the Philippine Sea, February 15, 2026. Marine F-35Bs bring a 5th generation multi-discipline strike capability to support combined-joint all domain operations in key maritime terrain. The 31st MEU is a persistent, combat credible force operating aboard the ships of the Tripoli Amphibious Ready Group in the U.S. 7th fleet area of operations, routinely interacting and operating with our allies and partners to contribute to deterrence, security, crisis response, and combat operations in the Indo-Pacific region. (U.S. Marine Corps photo by Lance Cpl. Victor Gurrola)

blacklisted tanker vessels and evade international sanctions.[21] Not only are internal, external, and ambient factors essential for characterizing an object in a domain, but they also aid in projecting future states.

Projection, the second aspect of sensemaking, extrapolates from the characterization of the environment and the objects it may contain, anticipates changes in that environment, and projects possible impacts of players' actions. Returning to the maritime domain, a U.S. Coast Guard cutter can anticipate another ship's intentions at sea from attributes such as its size, onboard equipment, and course. Moreover, by integrating information from other players, like a cargo manifest from U.S. Customs and Border Protection, the Coast Guard cutter could better anticipate the intent and subsequent actions of the cargo vessel. The Coast Guard applied this skill at least twice in 2024, joining partner nations to combat illegal, unreported, and unregulated fishing. First, a Coast Guard cutter joined with partner nations to prevent "a fleet of 800 Chinese vessels [from] plundering South America's fishing grounds [and avert an] environmental collapse."[22] Then, Coast Guard assets joined civil and military organizations from Japan, South Korea, and Canada to counter illegal fishing in the Pacific through "high seas patrols, air surveillance, and electronic monitoring."[23] The multiple information sources improved individual players' awareness and facilitated quick team sensemaking and action to build collaborative awareness to deter illegal fishing operations.

Accessibility of the range of observational and contextual data largely determines the simplicity or complexity of sensemaking. In the case of air domain awareness, commercial flights are well documented and monitored in the United States, giving air traffic controllers the requisite information to project weather impacts on the flights, for instance. In sharp contrast, incursions of unidentified drone swarms over and near Langley Air Force Base, Virginia, in 2024 demonstrate the limits of sensemaking—visual observations provided location, but lack of contextual data like aircraft ownership concealed intent.[24]

Collection capacity also affects analysis that supports sensemaking. In a domain overwhelmed by background noise, like a radar return in the air domain, established processes that once served to accelerate sensemaking may in fact hinder awareness. The Chinese balloon that traversed the United States in 2023 entered undetected into North American airspace. Early warning radars, calibrated to defend the homeland from bomber aircraft and missile attacks, were not calibrated to detect slow-moving objects. Rather than tracking every bird, piece of windswept debris, or balloon in the air, NORAD's systems were "filtering out that data," as General VanHerck stated. But tellingly, in that same interview General VanHerck warned that even though the United States requires better visibility into the Pacific, Arctic, and Atlantic regions to detect threats to the homeland, he is "most concerned about the cyber domain

and our ability to understand the threats in the cyber domain that impact [U.S.] power projection."[25]

Sensemaking consists of tools and processes to characterize and project actions based on visible factors in the domain environment. Because of the ever-expanding nature of the domain, sensemaking in cyberspace assuredly requires evolving technology and processes. Understandably, those advanced monitoring tools or developed cognitive processes will be distributed across industry and government players. Collating aspects of those capabilities in pursuit of common national security objectives requires well-defined shareability standards.

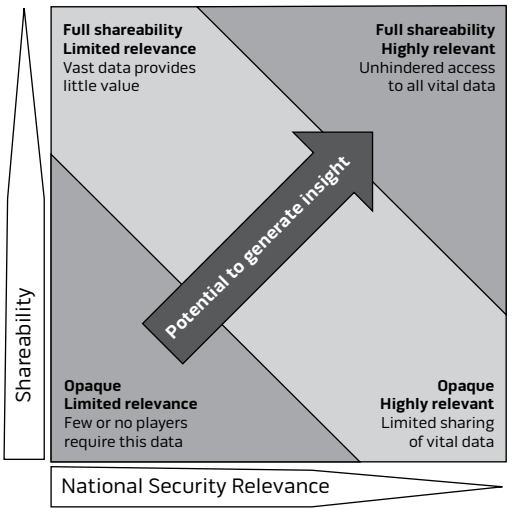
Shareability: Distributing Both Raw Data and Refined Analysis

The final principle necessary for collaborative awareness—shareability—predicates any unity of effort in cyberspace. Developing a shared, collaborative awareness for homeland cyber defense depends entirely on the ability to pass information among all players easily via agreed-upon pathways. This team includes players from across government and the private sector, as well as allies and partners who have roles in contributing to U.S. national security. A shared understanding of environmental factors enables not only collaborative awareness but also players' independent actions that contribute to a common goal.

Shareability in pursuit of collaborative cyber domain awareness does not translate as "radical transparency," but instead balances the competing interests or externalities for the team of players. Business gurus may argue that organizational performance is boosted when every organizational member knows all the details of every other member's work (that is, radical transparency).[26] However, that argument may not apply when team members share a common goal like national security but maintain competing objectives like increasing shareholder value or protecting proprietary material. Figure 4 illustrates the range of shareability and relevance to national security for potential data.

Different players will place the same data sets at various points in figure 4, depending on their situational awareness needs and the relevancy of the data. Case in point: weather data may be superfluous to one player but vital to another, while equally accessible to both. In general, the potential to leverage collaborative awareness to generate new insights will increase with greater shareability of data relevant to the problem set.

Figure 4.



Source: Authors.

Sharing efforts in other domains can be instructive here. The National Maritime Intelligence-Integration Office, for instance, pursues initiatives to "prevent intelligence and information gaps and to facilitate an effective understanding of the maritime domain."[27] Its initiatives seek to shepherd new relationships and engage with existing regional architecture to "improve access to common and interoperable maritime domain awareness data and tools" for stakeholder companies, government agencies, and international partners like INTERPOL.[28] For situational awareness in space, the U.S. Government shares basic data on potential satellite collisions and atmospheric reentries at no cost to users to enhance safety in space and support commercial development.[29] At the same time, DOW also advances efforts to integrate data from the growing space sensing industry. Recently, the U.S. Space Force prioritized efforts to share advanced, actionable threat information between DOW and the commercial sector.[30] The shared awareness enables commercial space operators to respond to threats and increases DOW's visibility and understanding of the space domain.

Inevitably, not all information can be shared freely, whether because of its classified sources or proprietary status. Two options should exist in these cases to maximize shareability while protecting various interests. One category of data would contain essential awareness data that is broadly sharable but pared of sensitive details, while a second version contains high-fidelity information for trusted partners. Again, the maritime and space domains provide examples of this information categorization. In the maritime domain, the Department of Transportation broadly transmits ship traffic data that other agencies could combine with unique information to build insightful threat awareness at various levels of releasability.[31] Space awareness data also has distinct levels of shareability. The Department of Commerce manages broadly available information on essential satellite orbital details and anomalies in one data set version. A second data set provides higher fidelity classified data to trusted government, international, and key industry space operators who require more details on specific threat behavior.[32] Commercial

partners also have valid concerns with information shareability, and a well-designed shareability framework should account for disparate equities.

From a cyber perspective, shareability is an essential but challenging element of developing collaborative awareness. The private sector broadly owns and operates cyberspace, and collaborative awareness is unachievable without broad industry participation. Now, private industry owns 85 percent of the U.S. infrastructure networks.[33] Likewise, over 90 percent of U.S. military and intelligence communications rely on commercial telecommunication networks.[34] Homeland security and defense efforts must integrate industry partners. Only by combining information and perspectives from all cyberspace players can a sense of domain-level awareness emerge to feed unity of effort. Shareability is especially important to counter adversaries campaigning to disrupt critical U.S. infrastructure and commercial networks. Because adversaries' actions may only be apparent after aggregating clues from multiple networks, shareability is a crucial principle of collaborative awareness.

Despite the shared need, there are innumerable policy, legal, and interest impediments to information sharing between government and private industry organizations. Some organizations have powerful business interests in not sharing broadly, such as regulatory effects or impacts to competitive advantage. For others, there are valid concerns about privacy protections for customer data and network traffic, which are significant considerations when sharing data with the government. Even producing something as basic as the cyber equivalent of Notices to Air Missions or Notices to Marines in a reliably consistent and timely way has yet to be achieved. The relatively slow march toward greater domain awareness may be due more to divergent interests and policies than to technical challenges.

In fact, some technological advancements may increase the possibility of a workable solution to shareability. Research in areas like anonymization produces new methods that aid collaborative awareness participation by allowing players to share relevant cyber defense information while lowering organizations' negative externalities and increasing the potential to generate domain insight.[35] As cyberspace evolves, a set of agreed-upon data standards will also benefit shareability. The 2018 National Space Traffic Management Policy emphasized common standards as a priority for space domain awareness as commercial sensing players and new data types continued to proliferate.[36]

The evolution of airspace awareness may also prove illustrative. Since 2020, the FAA has required aircraft to broadcast position and flight data via Automatic Dependent Surveillance-Broadcast (ADS-B) in most airspace to feed the FAA's monitoring systems. Since ADS-B data quality and speed outperform traditional radar returns, ADS-B information improves short-term aircraft trajectory projections. With this enhanced sensemaking, commercial carriers expanded domestic service in mountainous areas where radar could not provide coverage.[37] While not mandatory, aircraft can also receive ADS-B information directly from other aircraft instead of relying on a central actor like an air traffic controller to provide awareness. This federated shareability of information substantially increases aviation safety. For general aviation aircraft that were *broadcasting* ADS-B, accidents were reduced by 53 percent. Moreover, fatal accidents were reduced by 89 percent for aircraft *receiving* ADS-B information.[38]

Shareability must account for various players' perspectives and data needs. Air, maritime, and space domain awareness rely on accurate and timely information sharing to build awareness. As government and industry develop a collaborative awareness in cyberspace, shareability must be purposely crafted to support unity of effort for homeland defense.

Crafting Collaborative Awareness in Cyberspace

Regardless of the domain, homeland defense requires a shared awareness of activity in the environment to inform individual action and unify disparate efforts toward common objectives. Across domains, this awareness is best achieved through information sharing to enhance visibility and sensemaking by all players with roles in securing the domain. Against the apparent need for a shared understanding for cyberspace defense, a collaborative cyber awareness construct remains unrealized at the national level despite significant government and industry initiatives. U.S. national security leaders must thoughtfully organize public and private players and properly resource efforts to achieve collaborative awareness in the cyber domain in support of homeland defense.

While building collaborative awareness in cyberspace seems daunting, other domains may again prove enlightening regarding organizing and resourcing national-level awareness of a whole-of-nation domain. In particular, the development of NORAD's Semi-Automatic Ground Environment (SAGE) in the 1950s provides an example of a herculean effort to develop a shared awareness of a (then) cloudy domain. Early in the Cold War, NORAD lacked the awareness and command and control necessary to direct air defense efforts against a large-scale attack by nuclear-armed Soviet bombers. In response, the Department of Defense developed SAGE, a public-private national defense endeavor that eclipsed the Manhattan Project in cost and scale.[39] Used until 1984, SAGE linked hundreds of radar sites, control centers, U.S. military airfields, and surface-to-air missile sites to build NORAD's situational awareness and enable North American airspace defense: "It was far and away the most grandiose systems engineering effort—and the largest electronic system-of-systems 'ever contemplated.'"[40] Collaborative awareness for cyber defense does not require total information transparency or centralized control, tenets inherent to the design of SAGE. Instead, appropriate organization and well-defined roles can assist unity of effort for homeland defense.

To this end, the White House's Office of Science and Technology Policy (OSTP) could lead public and private entities to formulate a shared concept for collaborative awareness in cyberspace.

Already, OSTP leads nationally important initiatives like coordinating 13 Federal agencies and offices to explore quantum information science or synchronizing up to 35 public and private industry entities to draft responsible artificial intelligence policy.[41] No equivalent organization holds the attention of industry and academia while also maintaining access and influence over the whole of the U.S. Government and, to some extent, international partners. Of course, the Cybersecurity and Infrastructure Security Agency (CISA) would play a prominent role in authoring a concept for collaborative awareness, and the National Institute for Standards and Technology could referee technical standards underlying the visibility and shareability principles. Also, a properly structured nonprofit or quasi-public entity without regulatory authority could gain broader private sector participation, which is a challenge for current CISA initiatives, as evidenced by industry withdrawals from the Joint Cyber Defense Collaborative in late 2023 and early 2024.[42] To achieve consensus for a vision of collaborative cyber awareness, each player must also agree upon set roles and responsibilities.

DOW is critical in the collaborative awareness conversation because of its unique capabilities and equities. As with awareness in all other domains, DOW must be a key advocate for the homeland defense perspective in this cyber awareness effort. But first, the Pentagon must better define its homeland defense roles and responsibilities in cyberspace. To date, DOW is reluctant to become overly involved in largely private networks on American soil, resulting in an ill-defined line between homeland defense and homeland security. Undoubtedly, there are legal questions concerning military operations and the homeland, but cyberspace is detached from national borders, with its physical infrastructure and cyber effects spanning the globe. DOW understands homeland defense to start within the United States but extend to the nation's approaches and forward regions, just like cyberspace. To that end, DOW possesses unique authorities and capabilities, making it a powerful defensive partner. Unlike industry, the military can and does operate beyond the bounds of the virtual United States, even on adversary cyber terrain, to gain insight into or eliminate malign threat vectors.

DOW also maintains a national defense perspective that is unique among players. While other Federal agencies like DHS or CISA may offer opinions that align with DOW's perspective, only DOW can represent its defense equities. For instance, the growing risk to commercially owned critical infrastructure in the United States highlights the necessity of shepherding private and public capabilities for national security. Today, combatant commanders wonder aloud about the Nation's ability to project the joint force. The commander of U.S. Transportation Command, General Randall Reed, stated in his September 2024 Senate confirmation hearing that he would prioritize cyber resilience for broader logistics enterprise because the joint force "faces increasingly capable contests and disruptions in the air, land, sea, space, and cyberspace domains."[43] General Reed also noted the need for public-private partnership in the same hearing: "Since cyber is so connected between the government and the commercial world, having good quality relationships with the commercials is fundamental."[44] Developing collaborative awareness in cyberspace ahead of any serious conflict is essential to prevent disruptive attacks on critical U.S. infrastructure, which would negatively impact the military as well as Main Street.

Conclusion

Defeating large-scale, wartime cyberattacks on the homeland—and even mitigating ongoing day-to-day malign activity—requires awareness of the virtual battlefield to sense disturbance before disturbance and danger before danger, as Sun Tzu counseled. Given the nature of privately owned infrastructure and deep public-sector interest, developing the necessary level of collaborative awareness for homeland defense requires coordination between industry and government agencies.

Collaborative awareness acknowledges the interconnectedness of government and commercial networks and the independent goals of each player in cyberspace. The principles of visibility, sensemaking, and shareability all helped baseline awareness efforts in other domains and show promise in guiding future work in the cyber domain.

National security leaders can advance cyber collaborative awareness by developing proper organizational constructs, interagency roles, and resourcing. In turn, this shared understanding of cyber domain hazards enables government and private-sector organizations to detect and defeat critical cyber threats, achieving unity of effort for homeland defense. **JFQ**

Notes

[1] Cybersecurity and Infrastructure Security Agency (CISA), "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," CISA, February 7, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a; CISA, "Iranian Cyber Actors' Brute Force and Credential Access Activity Compromises Critical Infrastructure Organizations," CISA, October 16, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-290a; CISA, "Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure," CISA, September 5, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a.

[2] "2023 Global Threat Roundup Report: Trends in Cyberattacks, Exploits, and Malware," Forescout Research—Vedere Labs, January 24, 2024, https://www.forescout.com/resources/research-report_2023-threat-roundup, 4.

[3] Martin Matishak, "CISA's Top China Specialist Departs for Role at CIA," *The Record*, August 29, 2024, https://therecord.media/cisa-china-specialist-departs; Sarah Krouse et al., "China-Linked Hackers Breach U.S. Internet Providers in New 'Salt Typhoon' Cyberattack," *Wall Street Journal*, September 26, 2024, https://www.wsj.com/politics/national-security/china-cyberattack-internet-providers-260bd835.

[4] The U.S. budget for fiscal year 2025 alone allocated $27.5 billion across civilian and defense departments. See Office of Management and Budget, "Budget of the U.S. Government—Fiscal Year 2025," The White House, 2024, https://www.whitehouse.gov/wp-content/uploads/2024/03/budget_fy2025.pdf.

[5] *Hearing to Receive Testimony on the Posture of United States Northern Command and United States Southern Command in Review of the Defense Authorization Request for Fiscal Year 2024 and the Future Years Defense Program,*

Before the Senate Armed Services Comm., Subcomm. on Strategic Forces, 118th Cong., 1st sess., 9-10 (March 23, 2023) (statement of General Glen D. VanHerck, Commander, United States Northern Command and North American Aerospace Defense Command), https://www.armed-services.senate.gov/imo/media/doc/NNC_FY23%20Posture%20Statement%2023%20March%20SASC%20FINAL.pdf; Joint Cyber Defense Collaborative Act, H.R. 9768, 118th Cong., 2nd sess. (2024), https://www.congress.gov/bill/118th-congress/house-bill/9768/text. Emphasis added.

[6] Sean Atkins and Chappell Lawson, "An Improvised Patchwork: Success and Failure in Cybersecurity Policy for Critical Infrastructure," *Public Administration Review* 81, no. 5 (2021): 847–61, https://doi.org/10.1111/puar.13322.

[7] Section 1652 (Cyberspace Solarium Commission), John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, https://www.congress.gov/115/plaws/publ232/PLAW-115publ232.pdf.

[8] Cyberspace Solarium Commission (CSC), March 2020 CSC Report (Washington, DC: CSC, 2020), https://cybersolarium.org/march-2020-csc-report/march-2020-csc-report/; Jiwon Wa and Mark Montgomery, *2024 Annual Report on Implementation* (Washington, DC: CSC, 2024), https://cybersolarium.org/annual-assessment/2024-annual-report-on-implementation/.

[9] Joint Cyber Defense Collaborative Act, H.R. 9768, 118th Cong., 2nd sess. (2024), https://www.congress.gov/bill/118th-congress/house-bill/9768.

[10] *Unity of Effort Framework Quick Reference Pamphlet* (Washington, DC: The Joint Chiefs, 2013), 2, https://web.archive.org/web/20250823195221/https://www.jcs.mil/Portals/36/Documents/Doctrine/pams_hands/uef_qr.pdf.

[11] Christer Garbis and Henrik Artman, "Situation Awareness as Distributed Cognition," paper presented at the 9th European Conference on Cognitive Ergonomics, in *Proceedings of ECCE 1998—Limerick*, ed. T.R.G. Green et al. (Limerick, Ireland: European Association of Cognitive Ergonomics, 1998), 152, https://www.eace.site/Proceedings/ECCE%201998.pdf.

[12] M. Press, "Situation Awareness: Let's Get Serious About the Clue-Bird" (unpublished manuscript, 1986), quoted in Mica R. Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems," *Human Factors* 37, no. 1 (March 1995): 32, https://doi.org/10.1518/001872095779049543.

[13] Mica R. Endsley, "A Survey of Situation Awareness Requirements in Air-to-Air Combat Fighters," *International Journal of Aviation Psychology* 3, no. 2 (April 1993): 158, https://doi.org/10.1207/s15327108ijap0302_5.

[14] Paul M. Salmon et al., *Distributed Situation Awareness: Theory, Measurement, and Application to Teamwork* (London: CRC Press, 2017).

[15] Salmon et al., *Distributed Situation Awareness*, 10–11.

[16] Renée J. Stout et al., "Planning, Shared Mental Models, and Coordinated Performance: An Empirical Link is Established," *Human Factors* 41, no. 1 (March 1999): 61–71, https://doi.org/10.1518/001872099779577273.

[17] National Commission on Terrorist Attacks, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (New York: Norton, 2004), 25, https://govinfo.library.unt.edu/911/report/911Report.pdf.

[18] National Commission on Terrorist Attacks, *The 9/11 Commission Report*, 28.

[19] "Colombia: Potential Cocaine Production Increased by 53 Per Cent in 2023, According to New UNODC Survey," press release, United Nations Office on Drugs and Crime, October 18, 2024, https://www.unodc.org/unodc/press/releases/2024/October/colombia_-potential-cocaine-production-increased-by-53-per-cent-in-2023--according-to-new-unodc-survey.html; *The Coast Guard's Fiscal Year 2025 Budget Request, Before the Committee on Transportation and Infrastructure, Subcommittee on Coast Guard and Maritime Transportation*, 118th Cong., 2nd sess., May 23, 2024 (statement of Admiral Linda L. Fagan, Commandant, U.S. Coast Guard), https://www.congress.gov/118/chrg/CHRG-118hhrg56929/CHRG-118hhrg56929.pdf.

[20] Diego Laje and Nuray Taylor, "Narco-Subs: A Game of Hide-and-Seek," SIGNAL, June 1, 2023, https://www.afcea.org/signal-media/technology/narco-subs-game-hide-and-seek.

[21] Christoph Koettl, "How Illicit Oil Is Smuggled Into North Korea With China's Help," *New York Times*, March 26, 2021, https://www.nytimes.com/2021/03/24/world/asia/tankers-north-korea-china.html.

[22] "U.S. Coast Guard Supports Partner Nations' Fight Against Illegal Chinese Fishing," Diálogo Américas, June 25, 2024, https://dialogo-americas.com/articles/us-coast-guard-supports-partner-nations-fight-against-illegal-chinese-fishing.

[23] "U.S. Coast Guard, Canadian Forces, International Partners Wrap-Up Operation North Pacific Guard 2024," press release, United States Coast Guard News, October 29, 2024, https://www.news.uscg.mil/Press-Releases/Article/3949614/us-coast-guard-canadian-forces-international-partners-wrap-up-operation-north-p.

[24] Gordon Lubold et al., "Mystery Drones Swarmed a U.S. Military Base for 17 Days. The Pentagon Is Stumped," *Wall Street Journal*, October 12, 2024, https://www.wsj.com/politics/national-security/drones-military-pentagon-defense-331871f4.

[25] Patrick Smith, "Chinese Spy Balloon Exposed Gaps in U.S. Ability to Detect Threats, NORAD Commander Says," NBC News, July 20, 2023, https://www.nbcnews.com/news/us-news/chinese-spy-surveillance-balloon-flaws-threat-detection-norad-defense-rcna95094.

[26] Ryan Smith and Golnaz Tabibnia, "Why Radical Transparency Is Good Business," *Harvard Business Review*, October 11, 2012, https://hbr.org/2012/10/why-radical-transparency-is-good-business.

[27] "Maritime Information Sharing Initiatives," National Maritime Intelligence-Integration Office, https://nmio.ise.gov/Initiatives/Maritime-Information-Sharing-Initiatives/.

[28] "Maritime Information Sharing Initiatives."

[29] Donald J. Trump, memorandum, Space Policy Directive-3, "National Space Traffic Management Policy," *Federal Register* 83, no. 120 (June 21, 2018): 28973, https://www.federalregister.gov/documents/2018/06/21/2018-13521/national-space-traffic-management-policy.

[30] U.S. Space Force, *U.S. Space Force Commercial Space Strategy* (Washington, DC: Department of the Air Force, 2024), 12, https://www.spaceforce.mil/Portals/2/Documents/Space%20Policy/USSF_Commercial_Space_Strategy.pdf.

[31] "Data Statistics," Maritime Administration, U.S. Department of Transportation, updated August 2, 2023, https://web.archive.org/web/20230902142102/https://www.maritime.dot.gov/data-reports/data-statistics/data-statistics.

[32] Center for Strategic and International Studies, "Space Situational Awareness and Space Traffic Management Coordination Among U.S. Agencies," CSIS, November 17, 2020, https://youtu.be/BVSfBzmjCU8.

[33] Jeffrey F. Addicott, "Cyber Security and the Government/Private Sector Connection," *Pass It On* 21, no. 3 (Spring 2012): 1, https://commons.stmarytx.edu/facarticles/475.

[34] Adam Segal, "Bridging the Cyberspace Gap: Washington and Silicon Valley," *PRISM* 7, no. 2 (2017): 67, https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_7-2/prism_7-2.pdf.

[35] Jeremy Kepner et al., "What is Normal? A Big Data Observational Science Model of Anonymized Internet Traffic," arXiv e-prints (2024), https://doi.org/10.48550/arXiv.2306.09267.

[36] Trump, Space Policy Directive-3, 28970.

[37] Woodrow Bellamy III, "What's Next for ADS-B in the U.S. Air Traffic System?," Avionics International, accessed November 8, 2024, https://interactive.aviationtoday.com/whats-next-for-ads-b-in-the-us-air-traffic-system.

[38] Christian Ramsey, "Reducing Runway Incursions Isn't a $100M Problem. It's Much Less," *uAvionix* (blog), May 26, 2023, https://uavionix.com/reducing-runway-incursions-isnt-a-100m-problem-its-much-less.

[39] "SAGE: Semi-Automatic Ground Environment Air Defense System," Lincoln Laboratory Massachusetts Institute of Technology, accessed November 11, 2024, https://www.ll.mit.edu/about/history/sage-

semi-automatic-ground-environment-air-defense-system; Stephen Lukasik, "Why the ARPANET Was Built," *IEEE Annals of the History of Computing* 33, no. 3 (2011): 4–21, https://doi.org/10.1109/MAHC.2010.11.

[40] "SAGE."

[41] "Office of Science and Technology Policy," White House, accessed November 11, 2024, https://web.archive.org/web/20241111002538/https://www.whitehouse.gov/ostp/.

[42] Joseph Gedeon, "Cyber Pros Are Giving Up on a Key Government Program," Politico, February 5, 2024, https://www.politico.com/newsletters/weekly-cybersecurity/2024/02/05/cyber-pros-are-giving-up-on-a-key-government-program-00139540.

[43] *U.S. Transportation Command Nomination Hearing Before the* [Senate] *Comm. on Armed Services*, 118th Cong., 2nd sess., September 17, 2024 (stenographic transcript of hearing for the nomination of Lieutenant General Randall Reed, U.S. Air Force), 77, https://www.armed-services.senate.gov/imo/media/doc/nomination_hearing.pdf.

[44] *U.S. Transportation Command Nomination Hearing Before the Committee on Armed Services*, 88.