TESTIMONY
OF
ARIEL A. DEJESUS, JR
DEPUTY DIRECTOR
NATIONAL SECURITY DIVISION
THE AMERICAN LEGION
BEFORE THE
HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON CYBER, INFORMATION TECHNOLOGIES, AND INNOVATION
ON
"INDUSTRY VIEWS ON PARTNERSHIP WITH THE DEPARTMENT OF DEFENSE AND THE DEFENSE INDUSTRIAL BASE"

JUNE 2025

TESTIMONY
OF
ARIEL A. DEJESUS JR
DEPUTY DIRECTOR
NATIONAL SECURITY DIVISION
THE AMERICAN LEGION
BEFORE THE
HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON CYBER, INFORMATION TECHNOLOGIES, AND INNOVATION
ON
"INDUSTRY VIEWS ON PARTNERSHIP WITH THE DEPARTMENT OF DEFENSE AND THE DEFENSE INDUSTRIAL BASE"

JUNE 2025

Introduction

Chairman Bacon, Ranking Member Khanna, and distinguished members of this Subcommittee, on behalf of National Commander James LaCoursiere Jr., and more than 1.5 million dues-paying members of The American Legion, we thank you for the opportunity to offer our testimony for the record.

The American Legion is guided by active Legionnaires who dedicate their time and resources to serve veterans, servicemembers, their families, survivors, and caregivers. As a resolutions-based organization, our positions are directed by more than 106 years of advocacy and resolutions that originate at the post level of our organization. Every time The American Legion testifies, we offer a direct voice from the veteran community to Congress.

I want to thank you and the members of this Subcommittee for unswervingly supporting our nation's uniformed service members, veterans, and their families. As an organization of veterans and service members who have fought for our freedoms, The American Legion believes the national security of the United States of America is upheld by maintaining a well-funded Department of Defense (DOD), an excellent quality of life for troops, and a sensible transition between service and separation. We also believe that the current National Defense posture emphasizes the need for a strong and capable military force to meet various challenges, from great power competition to emerging technologies and non-state actors.

Although every domain of warfare requires close attention, especially as our country faces near-peer competitors, the cyberspace domain has proven to be uniquely important. Cyberattacks are on the rise as federal, state, and local governments have seen a startling number of attacks on public infrastructure, both government and commercial.[1] Hackers closely aligned with countries like Russia and China, as well as transnational criminal organizations, have targeted everything from food and water supplies to enterprise software programs that Americans rely on daily.[2] These attacks represent an emerging threat that can only be addressed by a comprehensive cyber framework. No other entity is as capable of fighting back as DOD. This is why our members believe that Congress should provide DOD with the resources they need to research, develop and field advanced technologies to defend the American people from these malicious attacks.

A strong and resilient Defense Industrial Base (DIB) is vital to our national security. Like any complicated weapon system or platform that is vital to positive effects on the battlefield, tools that increase our cyber-readiness will require our government's investment in extensive resources and time to field, equip, and train our cyber-operators and organizations for successful employment. This is why it is crucial to send strong demand signals to the private sector to jumpstart the developmental pipeline for these tools. Leveraging defense and private industrial partner's expertise is essential to remaining nimble and innovative.

Background and The American Legion's Relevant Work

One of The American Legion's four pillars is National Security, and we maintain resolutions specifically focused on ensuring a lethal fighting force and protecting national security. Resolution No. 25: *Funding for Protection of the National Power Grid Against Electromagnetic Pulse Attack* supports adequate funding to protect the deteriorating United States power grid, which remains vulnerable to electromagnetic pulses (EMP) and high-altitude electromagnetic pulses (HEMP) from adversaries such as Russia, China, and non-state actors. Without continued efforts to defend the power grid, military and civilian electronic communication systems and operational capabilities will be compromised, weakening the United States' national security. By investing in cyber defenses for the power grid, the U.S. ensures a robust and sustainable DIB.

Resolution No. 48: *Rebuilding the U.S. Defense Industrial Base* calls for revitalizing the DIB, emphasizing the need to modernize production capacity, reinforce supply chains, and grow a skilled defense industrial workforce. Without such investment, the U.S. risks compromising its ability to deter, respond to, and prevail in major conflicts - both cyber and conventional. The DIB

[1] David Jones. "Critical Infrastructure at State, Local Levels at Heightened Risk of Cyberattacks." Cybersecurity Dive. February 28, 2025. https://www.cybersecuritydive.com/news/critical-infrastructure-state-local-cyber/741273/.
[2] David Klepper. "Cyber Criminals Are Increasingly Helping Russia and China Target the US and Allies, Microsoft Says." AP News. October 15, 2024. https://apnews.com/article/microsoft-russia-china-iran-israel-cyberespionage-cyber-d3a22dd2dcea32615ac15ed4fb951541.

serves as the foundation of America's military strength and a core pillar of its strategic autonomy and national resilience.

Resolution No. 7: *Rebuilding the Civil-Military Relationship in America* calls on DOD to rebuild public trust in the military by promoting the societal value of national service. One way to achieve this is by encouraging the hiring of veterans in the private sector to work and collaborate across the DIB.

Resolution No. 20: *National Cybersecurity Strategy* highlights the rapid evolution of digital capabilities within defense infrastructure and the government increasing reliance on the cyber domain for many essential functions. The resolution calls for a national cybersecurity strategy that includes building partnerships among public and private organizations, interagency coordination, establishing mechanisms and incentives to encourage routine information sharing for collective defense, and educating users about their role in thwarting cyberattacks.

Resolution No. 338: *Support Licensure and Certification of Servicemembers, Veterans and Spouses* supports efforts to eliminate employment barriers that hinder the timely and successful transfer of military job skills to the civilian labor market, as well as to remove employment obstacles for spouses through advocacy for the recognition and acceptance of their professional credentials.

Resolution No. 15*: Department of Defense Issuance for Military Credentialing Programs s*upports a seamless transition of servicemembers into the civilian workforce, urging DOD to eliminate obstacles to transferring military credentials into civilian certifications by creating consistency and uniformity across all service branches. DOD is encouraged to establish baseline requirements for military credentialing programs to all military branches. Leveraging public-private partnerships helps accelerate this process by aligning military training standards with industry-recognized certifications in the DIB, ensuring that servicemembers' hard skills are recognized and easily transferable.

Resolution No. 33: *Rare Earth Elements* urges DOD to provide regular assessments of rare earth supply-chain requirements and calls on the Secretary to maintain a long-term rare-earth element supply plan. Given China's dominant position in the rare earth element market and its potential to exploit this leverage to influence U.S. foreign policy, it is essential to reduce dependency through diversified sourcing and strengthened domestic capability. Public-private partnerships play a critical role in this effort, fostering collaboration in research and investment.

The *FoRGED Act*

The *Fostering Reform and Government Efficiency in Defense (FoRGED) Act,* led by Senator Roger Wicker (R-MS), is an essential piece of legislation that could further advance the defense

capabilities of the DIB through simplifying regulations and reporting requirements, elevating commercial contracting, cutting red tape, providing budget flexibility, and fostering cooperation for defense procurement.[3]

From a cybersecurity and innovation perspective, leveraging the technological expertise of the private sector is essential to developing effective DOD cyber programs. While DOD and other public sector agencies have immense capabilities to integrate emerging technologies, they are not capable of the same iterative progress and development as the private sector.

This bill aims to leverage the private sector's competitive pressure by simplifying qualification and testing procedures and broadening the pool of eligible participants. It calls for modernizing the budgeting process to enhance agility and transparency in resource allocation and execution.[4] The bill reduces the administrative burden on both traditional and non-traditional defense contractors by streamlining regulations and reporting requirements. This makes it easier for private companies to enter and compete in the defense marketplace. As a result, this broader base of participation drives innovation and resilience across the industrial base, increasing productivity and strengthening cyber defense.

The American Legions supports the *FoRGED Act* through Resolution No. 48, *Rebuilding the U.S. DIB* which emphasizes the urgent need to modernize and secure the domestic defense manufacturing sector to enhance national readiness and reduce reliance on foreign suppliers. The *FoRGED Act* advances these goals through strategic federal investments in critical production areas such as semiconductors, munitions, and rare earth elements, while also promoting workforce development initiatives that benefit transitioning veterans. Crucially, the bill would reinforce public-private partnerships and innovation- core principles of Resolution No. 48- to strengthen supply chain resilience and ensure the long-term sustainability of the U.S. DIB.

The *SHIPS for America Act*

The American Legion strongly supports legislative efforts to restore and build up the United States' maritime capabilities. This will provide enhanced shipping capacity, both commercial and military- and expand America's physical footprint in global oceans. Increasing our physical posture around the world will also extend our cyber, information, and technological platforms globally. This presence will deter aggression abroad, empower our cyber capabilities, and enhance U.S. economic security.

---

[3] "Text - S.5618 - 118th Congress (2023-2024): FoRGED Act." 2024. Congress.gov. December 16, 2024. https://www.congress.gov/bill/118th-congress/senate-bill/5618/text/is.
[4] Michael Brown. 2025. "Memo to Congress: Pass the FoRGED Act." Forbes. February 7, 2025. https://www.forbes.com/sites/mikebrown/2025/02/07/memo-to-congress-pass-the-forged-act/.

The American Legion proudly supports the *Shipbuilding and Harbor Infrastructure for Prosperity and Security (SHIPS) for America Act*, led by Senators Mark Kelly (D-AZ) and Todd Young (R-IN), and Representatives Trent Kelly (R-MS) and John Garamendi (D-CA). This vital piece of legislation is crucial to strengthening our shipbuilding industry, fostering maritime readiness, and enhancing our commercial maritime presence overseas, all of which will significantly improve our cyber programs and workforce.

The *SHIPS for America Act* establishes an ambitious yet critical goal: to grow the number of U.S.-built, U.S.-flagged, and U.S.-crewed commercial ships from around 80 to at least 330 vessels within the next 10 years.[5] This growth is necessary, not just to build a a robust maritime fleet, but also to ensure that capable sealift capacity and logistical support infrastructure are available for military operations in future conflicts.[6] Crucially, it will also provide a physical deterrence option to information warfare operations by our adversaries- such as the Russia-linked ships cutting underwater cables in the Baltic Sea and other European waters.[7]

The American Legion's Resolution No. 29: *Commercial Shipbuilding for Defense* urges the President and Congress to raise maritime budgets, spur commercial shipbuilding, expand the use of U.S.-flagged ships in international trade, and respond to foreign actions. A robust commercial fleet and shipbuilding industry are not merely economic necessities; they are stalwarts of our national defense complex.

Ships are no longer simply about steel and propulsion. They are about systems integration, software, and cyber protection. Modern ships are sophisticated, cyber-physical platforms, reliant on digital controls, navigation software, satellite communications, and onboard information systems that must be hardened against cyberattacks. A cyberattack aboard a warship or within the industrial control network of a shipyard could compromise operations, expose sensitive data, and paralyze strategic mobility.[8]

Moreover, the cybersecurity of the shipbuilding supply chain- including critical elements in navigation systems, satellite communications, and onboard control software- must be regarded as a core national security concern. The use of foreign-made electronics, particularly those made from adversaries, throughout commercial shipping presents risks of embedded vulnerabilities and

---

[5] Shipbuilding and Harbor Infrastructure for Prosperity and Security for America Act of 2025. S. 1541/H.R. 3151. S.1541 - 119th Congress (2025-2026): A bill to support the national defense and economic security of the United States by supporting vessels, ports, and shipyards of the United States and the U.S. maritime workforce. | Congress.gov | Library of Congress

[6] Modern War Institute. "Cyber at Sea: Protecting Strategic Sealift in the Age of Strategic Competition." *Modern War Institute at West Point*, September 21, 2023. https://mwi.westpoint.edu/cyber-at-sea-protecting-strategic-sealift-in-the-age-of-strategic-competition/.

[7] "Europe's New War with Russia: Deep Sea Sabotage." POLITICO, April 2025. Europe's new war with Russia: Deep sea sabotage – POLITICO

[8] Burrell, Jessica A. 2023. "The Navy Still Suffers from Cybersecurity Complacency." Proceedings, March. https://www.usni.org/magazines/proceedings/2023/march/navy-still-suffers-cybersecurity-complacency.

potential remote compromise.[9] Doubling the number of U.S.-built and U.S.-crewed ships significantly reduces these risks while contributing to ensuring the safe, sovereign control of the most vital maritime platforms in both peacetime and in war.

Finally, the reinforcement of domestic shipbuilding infrastructure directly benefits the DIB's resilience and ability to recover from cyberattacks. Investments sought in the *SHIPS for America Act,* such as shipyard modernization, tax credits to facilities, and establishment of a Maritime Security Trust Fund, also improve cyber infrastructure upgrades, worker training, and digital integration required for secure operation of modern shipyards.

The American Legion urges the Subcommittee on Cybersecurity to consider shipbuilding not only as a manufacturing necessity but also as a cyber defense imperative. While our ships carry America's national security interests abroad, the systems that build and maintain them must be secured against cyber-attack here in the homeland. Additionally, building out the industrial capacity to produce ships improves our country's ability to integrate cyber platforms into the maritime fleet and provides physical platforms that enable and support our cyber and information strategies.

Revitalizing America's DIB: The Role of Public-Private Partnerships, Workforce Development, and Strategic Innovation

Enabling Success Through Public-Private Partnerships

A strong and resilient DIB is vital to national security and military readiness. The *FoRGED Act*, particularly Sections 315–317, underscores the importance of public-private partnerships by promoting nontraditional defense contracting and accelerating the acquisition process. Collaboration between DOD and industry is essential to rapidly increase production capacity, strengthen supply chains, foster innovation, and develop a skilled defense workforce. The American Legion's Resolution No. 48 also emphasizes strengthening public-private partnerships to enable rapid industrial mobilization.[10] Thus, this partnership has the potential to fill knowledge gaps and allows for an exchange of information that the Pentagon may not have. Furthermore, those same partnerships will give DOD a better understanding of industry dynamics and workforce capabilities. Unlike the federal government, private companies often do not face the same bureaucratic hurdles as federal agencies. This allows them to work quickly as technologies such as artificial intelligence (AI), advance rapidly.

[9] "Guide to Ship Cybersecurity." Maritime Institute of Technology and Graduate Studies, March 2024. Ship Cybersecurity | Maritime Industry Cybersecurity

[10] "Resolution No. 48: Rebuilding the U.S. DIB | Digital Archive." 2023. Legion.org. The American Legion. August 2023. https://archive.legion.org/node/15097.

Advancing Workforce Development and Veteran Integration

The American Legion strongly believes that Congress should increase workforce development programs to credential more workers and veterans for high-demand trades to rebuild the DIB.[11] The American Legion strongly supports the *Defense Workforce Integration Act* led by Senator Jeanne Shaheen (D-NH) in the Senate and Representative Jen Kiggans (R-VA) in the House. This initiative supports veteran employment by translating military-acquired skills into civilian opportunities, reinforcing the value of service. It also strengthens recruitment by assuring future service members that their expertise will be recognized and utilized beyond active duty, aligning with DOD efforts to expand public-private partnerships and veteran engagement, as outlined in Resolution No. 7: *Rebuilding the Civil-Military Relationship in America.*

Task Force Movement (TFM), a White House-supported initiative, was launched with the goal of fast-tracking veterans, transitioning service members, and their families into civilian careers in fields such as cybersecurity. The American Legion along with other organizations support the initiative, recognizing the TFM's prominent role in facilitating veterans' entry into essential industries. TFM engages in strategic collaboration with industry experts and government agencies to create sustainable, high-quality career pathways for veterans, transitioning service members, and military families. With a focus on sectors facing critical workforce needs, such as cybersecurity, TFM supports veterans' transition to civilian employment and contributes to strengthening the nation's infrastructure and security.[12] To ensure that the DIB is actively supported through this task force, TFM works to provide scholarships and accelerated training programs to participants.[13] Veterans who obtained licenses and certifications while in the military and are seeking work in the defense sector often face barriers to entry. This led to The American Legion's efforts surrounding Resolution No. 15: *Department of Defense Issuance for Military Credentialing Programs.*

Countering Global Competitors Through Technological Superiority

The *FoRGED Act,* aligned with The American Legion's Resolution No. 48, stresses the importance of strengthening the DIB to enhance U.S. national security mechanisms. The United States is facing growing threats from near-peer adversaries and history shows that wars between major powers often expand into protracted conflicts.[14]

---

[11] "Resolution No. 48: Rebuilding the U.S. DIB | Digital Archive." 2023. Legion.org. The American Legion. August 2023. https://archive.legion.org/node/15097.
[12] "Cyber Security - Task Force Movement." Task Force Movement. December 18, 2023. https://taskforcemovement.org/cyber-security/.
[13] "Task Force Movement Continues to Evolve." The American Legion, June 24, 2024. https://www.legion.org/information-center/news/careers/2024/june/task-force-movement-continues-to-evolve.
[14] "Resolution No. 48: Rebuilding the U.S. DIB | Digital Archive." 2023. Legion.org. The American Legion. August 2023. https://archive.legion.org/node/15097.

On U.S. Inauguration Day in 2025, China released its AI language model, DeepSeek, signaling China's AI capabilities are approaching parity with the United States. As a result, China's potency in AI raises national security concerns, as dual-use technologies like AI have considerable military applications.[15]

With China and Russia producing cutting-edge technological systems, it underscores the need for the U.S. to rapidly deploy more technological innovation across its defense sector. To maintain its edge, the U.S. must ensure that DOD can iteratively acquire and field emerging technologies at the same pace as commercial innovation. Otherwise, the U.S. will see its competitors, such as China increase their technological capabilities faster than the U.S.[8] Moreover, not maintaining a technological advantage over adversaries raises significant concerns regarding the strategic balance of power. Should China surpass the United States in advanced technologies and artificial intelligence, it could expand its ever-present influence in global affairs, particularly in regions of strategic interest to the United States.[16]

An increase in near-peer technological superiority can erode U.S. influence with key partner nations and potentially create a power vacuum that would undermine regional stability. This situation is particularly alarming given the presence of vital U.S. military installations in East Asia, including in Japan and the Republic of Korea, where maintaining a credible deterrence is essential to our national security and that of the region.[17]

Problem Areas

Cyber-Attacks

Cyber-attacks significantly impact civilian infrastructure, including essential services and commercial software. Historically, cyber-attacks from near-peer adversaries have targeted state and local governments and have affected food and water services, financial systems, and informational websites. Local governments remain particularly vulnerable to these attacks, as they often lack the technological sophistication to protect their systems. These attacks put domestic power grids at risk, which could have deep impacts on American communities and local economies. Such attacks have been prevalent in Ukraine's war with Russia and have caused considerable harm to civilian populations inside Ukraine and across Europe. Congress and DOD should view these examples as a warning of what could occur if the U.S. is not adequately prepared.

---

[15] Michael Brown. 2025. "Memo to Congress: Pass the FoRGED Act." Forbes. February 7, 2025. https://www.forbes.com/sites/mikebrown/2025/02/07/memo-to-congress-pass-the-forged-act/.
[16] Cole McFaul and Peter Engelke. "Navigating the US-PRC Tech Competition in the Global South." Atlantic Council. April 16, 2025. https://www.atlanticcouncil.org/in-depth-research-reports/report/navigating-the-us-prc-tech-competition-in-the-global-south/.
[17] U.S.-China Economic and Security Review Commission, 2023 Annual Report to Congress, Chapter 3: "China's Defense and Military Capabilities in AI and Emerging Technologies."

Cybersecurity is not solely a federal concern but a shared responsibility across government, industry, and the public. Today's digital ecosystem supports nearly every aspect of American life. Cyber-attacks are on the rise and continue to place national security at risk. In 2023, the MOVEit cyber-attack, based out of the United Kingdom, compromised multiple U.S. agencies at both the federal and state levels.[18] Constant threats from our adversaries like China, Russia, North Korea, and Iran underscores the scale and growing sophistication of cyber operations directed at the U.S. and its partners. These incidents reinforce Resolution No. 20's call for interagency and commercial coordination to build cyber resilience.

In response to these phenomena, the White House, in January of this year, released an executive order to strengthen U.S. cybersecurity by requiring transparency and security in third-party software supply chains. This strengthened the security of federal communications, improved accountability for software and cloud service providers, and promoted security with AI by launching public-private partnerships for cyber defense in the energy sector.[19]

The Concerning Rise of Artificial Intelligence and DOD Response

With AI becoming more prevalent across multiple sectors, DOD must learn to evolve by using AI as a defense mechanism. The DIB faces the added danger of asymmetric attacks, which further necessitates public-private collaboration. THUNDERFORGE is a program created by the Defense Innovation Unit which tests and analyzes military operational power to identify better planning techniques and policies.[20] Scale AI, a private company, has maintained a strong partnership with DOD to develop AI-driven military operations and simulations. To counter cyber-attacks and China's accelerated AI deployment, Scale AI and DOD must determine AI concepts and assess their effects on our adversaries. Adopting new acquisition pathways to enable DOD to move quickly is also vital. Scale AI supports DOD in using AI effectively by reinforcing access to critical AI infrastructure, such as the Cloud.[21] Thus, the implementation of AI tools developed through government and industrial partnerships could help DOD close our gap in information capabilities.

---

[18] Carly Page. "MOVEit, the Biggest Hack of the Year, by the Numbers." TechCrunch. August 25, 2023. https://techcrunch.com/2023/08/25/moveit-mass-hack-by-the-numbers/.

[19] The White House. "FACT SHEET: New Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity | the White House." The White House. January 15, 2025. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2025/01/15/fact-sheet-new-executive-order-on-strengthening-and-promoting-innovation-in-the-nations-cybersecurity/.

[20] Jason Miller. "DoD Modernization Exchange 2025: Google's Scott Frohman on Restoring Symmetry to the Cyber Fight." Federal News Network - Helping Feds Meet Their Mission. Federal News Network. March 28, 2025. https://federalnewsnetwork.com/federal-insights/2025/03/dod-modernization-exchange-2025-googles-scott-frohman-on-restoring-symmetry-to-the-cyber-fight/.

[21] "Scale AI's Alexandr Wang on Securing U.S. AI Leadership." Csis.org. Center for Strategic and International Studies. May 1, 2025. https://www.csis.org/analysis/scale-ais-alexandr-wang-securing-us-ai-leadership.

A Vulnerable Power Grid and Energy Sources

U.S. defense officials have described EMPs as massive "energy waves" that have the potential to destroy satellites that the U.S. and the international community depend on. One orbital blast could instantaneously knock out military and civilian satellites that are critical to GPS navigation, telephone lines, internet links, financial transactions, and cybersecurity mechanisms. EMPs constitute a major threat to U.S. national security. DOD's manual entitled "The Effects of Nuclear Weapons" describes EMPs consisting of three distinct pulse components known as E1, E2, and E3. The detonation sequence and effects from each of these components vary, as "each can cause damage which can allow subsequent components to cause greater damage than they might independently." In addition to disrupting civilian and military communications, defense systems that utilize global navigation systems would also be affected, leaving the U.S. in a vulnerable position. Power grids are particularly attractive targets for malign actors, as such disruptions could impact a command-and-control centers' ability to function.[22]

EMP damage to the energy sector, specifically the electrical grid, would negatively impact the United States' telecommunication, banking and finance systems, petroleum and natural gas, water, transportation, emergency services, space control; possibly impacting the continuity of government. A HEMP or Super EMP weapon can inflict an incredible amount of damage on U.S. critical infrastructure. Due to the lack of current investment to harden our most critical infrastructure, this type of damage could be long-lasting.[23] The U.S. must enhance its public-private partnerships in its infrastructure sectors to increase its resiliency and reduce potential recovery time. Due to its reach and footprint, DOD is the best place to start this process.

Much of the United States' critical infrastructure, such as energy production and distribution, telecommunications, and financial systems, is owned and operated by private companies. As a result, any comprehensive effort to safeguard energy and the power grid must involve collaboration between DOD and private industry. Public-private partnerships help bridge the gap between federal policy and commercial execution. By aligning knowledge, pooling resources, and leveraging capabilities, these partnerships can deploy EMP-resilient technologies more quickly, create standardized protocols, and enhance response and recovery planning. Ultimately, this partnership will serve as a force multiplier for U.S. national security, ensuring that the nation's infrastructure remains proactive in addressing evolving risks.

---

[22] Zhanna L. Malekos Smith. "The Specter of EMP Weapons in Space." Carnegiecouncil.org. Carnegie Council for Ethics in International Affairs. March 27, 2024. https://www.carnegiecouncil.org/media/article/the-specter-of-emp-weapons-in-space.

[23] Christopher Colyer. "The Threat of Nuclear Electromagnetic Pulse to Critical Infrastructure HS Today." HSToday. May 15, 2023. https://www.hstoday.us/subject-matter-areas/infrastructure-security/the-threat-of-nuclear-electromagnetic-pulse-on-critical-infrastructure/.

Space and Cybersecurity Policy

The cyber domain is also intrinsically connected to the space domain. In 2022, Russia conducted a cyberattack against a California-based provider of high-speed satellite broadband that served the Ukrainian military. Many of the services targeted by cyber-attacks are facilitated by satellites, making space an emerging theater for these types of attacks. In fact, the U.S. Space Force is highly focused on the information operations that impact the space domain, and cyber warfare has continued to be a primary focus of the service.[24]

Russia has effectively damaged fundamental elements of space infrastructure as part of its full-scale invasion of Ukraine. Russia is regularly jams navigation, positioning, and timing systems, which severely impact military operations and raises the risk for civilian aviation. Russia is also jamming communications satellites in space, demonstrating effective cyber capabilities against space-enabled communications.[25] These malicious attacks against space resources are likely to increase in frequency and intensity in the future. The U.S. DIB can counter these attacks in much the same way as with cyber-attacks; by increasing public-private partnerships and strengthening strategic communication, and expanding information- and resource-sharing.

Perhaps the greatest danger in this area would be the deployment of a nuclear weapon in space. If an adversary were to disable U.S. early-warning satellites or disrupt military communication links, it could cripple the United States' ability to observe threats to cybersecurity and coordinate forces. The risk of uncontrolled escalation is extremely high, as crossing the nuclear threshold in space would likely lead to a rapid chain of reprisals. The existence of a Russian orbital nuclear capability could be intended to sow uncertainty and deter Western support for allied states, such as for Ukraine. This introduces a new kind of arms race into international cybersecurity.[26]

Against this backdrop, the space policy domain is undergoing unprecedented growth, driven by a surge in government and private activities. Private investments in space have increased dramatically, with companies such as SpaceX, OneWeb, and Orbital Insight planning the launch of thousands of new satellites, ground infrastructure, and intelligence-gathering services. Government activity in space has also expanded with approximately 60 countries investing in new space capabilities, making space a crowded environment for policy. As a result, the risk of

[24] John J. Klein. "Space and Cyber Warfare as One." Csis.org. Center for Strategic and International Studies. October 31, 2024. https://www.csis.org/analysis/space-and-cyber-warfare-one.
[25] Bruce McClintock and Anca Agachi. "NATO Space Enterprise: Throttle up or Fall Short." Rand.org. Defense News. June 4, 2024. https://www.rand.org/pubs/commentary/2024/06/nato-space-enterprise-throttle-up-or-fall-short.html.
[26] "Orbiting Armageddon: Russia's EMP Threat from Space and Transatlantic Responses – INSIGHT EU MONITORING." 2025. Ieu-Monitoring.com. Insight EU Monitoring. April 17, 2025. https://ieu-monitoring.com/editorial/orbiting-armageddon-russias-emp-threat-from-space-and-transatlantic-responses/609700?utm_source=ieu-portal.

mismanagement has heightened. Thousands of satellites relying on overlapping frequency bands raise issues of signal interference and overall, degraded system performance. [27]

As the number and complexity of space actors grow, current U.S. governance structures may struggle to keep pace with this rapidly evolving landscape. Consequently, the DIB should address this issue by conducting strategic dialogue to promote interoperability standards with private-sector partners, ensuring that systems can operate cohesively in contested and congested cyberspace environments. Sharing and discussing technical protocols can serve as a deterrent to adversaries by enhancing collective resilience against cyberattacks in space. Partnering with private companies allows the U.S. DIB to rapidly integrate advanced cyber capabilities, increasing the DIB's responsiveness and effectiveness in a rapidly evolving space domain.

Strengthen Supply Chain Resiliency

As the war in Ukraine demonstrates, industrial capacity, production, and logistical/supply chain security are crucial for victory in modern warfare.[28] Mineral supply chains that are essential to technological devices and hardware are especially vulnerable to disruption, as the U.S. disproportionately depends on imports. If imports were shut off, the U.S. government would have difficulty producing too many critical items.[29] The U.S. defense industry must increase its supply chain resiliency and reduce its reliance on foreign countries. This could include reshoring production of key components, stockpiling critical materials, and expanding domestic industrial capacity.

In addition to physical supply chain vulnerabilities, there is an urgent concern regarding cyber dependencies and vulnerabilities due to the widespread integration of foreign technologies within the U.S. DIB. Roughly one-third of the U.S. supply chain depends on software or services from companies labelled by DOD as "Chinese Military Companies," while two-thirds of the supply chain depends on firms with suspected ties to China-linked entities. Despite increasing national security concerns, Chinese military-linked companies remain rooted in the U.S. digital supply

[27] Stephen Ganote, et al. "Reenergizing Transatlantic Space Cooperation: Opportunities in Security and Beyond." Atlantic Council. October 1, 2019. https://www.atlanticcouncil.org/in-depth-research-reports/report/reenergizing-transatlantic-space-cooperation-opportunities-in-security-and-beyond/.
[28] "Resolution No. 48: Rebuilding the U.S. DIB | Digital Archive." 2023. Legion.org. The American Legion. August 2023. https://archive.legion.org/node/15097.
[29] Sandra R. Thomas 2025. "VIEWPOINT: DIB Sector Won't Surge without Policy Changes." Nationaldefensemagazine.org. National Defense Industrial Association. April 7, 2025. https://www.nationaldefensemagazine.org/articles/2025/4/7/defense-industrial-base-sector-wont-surge-without-policy-changes.

chain. This dependency raises concerns about espionage, data security, and systemic risk.[30] The U.S. government must evaluate its supply chain relationships and proactively address associated cyber risks.

Most defense contractors use legacy IT systems or rely on poorly secured third-party providers, opening doors to potentially debilitating cyberattacks that can halt production, pilfer sensitive data, and disrupt logistics. Legacy systems typically lack enhanced security features, which makes them easy targets for bad actors. Adversaries can exploit these weaknesses to disrupt production lines, defense technologies, battlefield preparedness, and steal valuable intellectual property, including weapons designs and command-and-control software.

The DIB ecosystem's interconnectivity and complexity-spanning from Tier 1 contractors all the way to small suppliers- also amplifies the issue, since the vulnerability at one node can spread across the entire chain. The software supply chain is of particular concern, as code or firmware can be injected into the development or maintenance cycle and spread quickly. Such attacks, like the SolarWinds attack, have demonstrated the scope and the subtlety with which attackers can invade trusted platforms without detection for months.

DOD must harden cybersecurity practices with multi-layered defense frameworks among defense contractors, both large and small. This requires the implementing zero-trust architectures that validate every user and every device, every time; employing ongoing AI-driven anomaly-based monitoring; and conducting regular red-teaming and penetration testing drills to uncover and repair vulnerabilities. Expanding public-private threat intelligence sharing, as done in the Defense Industrial Base Cybersecurity Program (DIB CS), will help reduce response times. Funding programs, technical support initiatives, and compliance models- such as the Cybersecurity Maturity Model Certification- must also be streamlined and enforced.

Ultimately, the cybersecurity resiliency of the U.S. Defense Industrial Base is not only a question of technicalities but also one of strategic deterrence. A digitally hardened DIB ensures continuity of operations, secures technological superiority, and dissuades adversaries from attempting attacks in the first place due to the high probability of detection and failure.

[30] Anna Ribeiro. “Bitsight TRACE Reports Cyber Risks in US Supply Chains due to Foreign Providers.” Industrial Cyber. March 18, 2025. https://industrialcyber.co/supply-chain-security/bitsight-trace-reports-cyber-risks-in-us-supply-chains-due-to-foreign-providers/.

Conclusion

Chairman Bacon, Ranking Member Khanna, and distinguished members of the Subcommittee, The American Legion thanks you for your leadership on these important issues and for allowing us the opportunity to provide our position and recommendations.

The American Legion believes revitalizing the U.S. Defense Industrial Base and increasing cyber capabilities is essential to national security and global stability. As outlined in Resolution No. 48, America's military strength depends on modernized production capacity, robust supply chains, workforce development, technological innovation, and strong public-private partnerships. We urge Congress to act swiftly to reinforce the DIB foundation, invest in skilled veteran labor, and promote partnerships that ensure America's enduring cyber and military readiness.

Questions concerning this testimony can be directed to Bailey Bishop, Senior Legislative Associate, at b.bishop@legion.org.