TESTIMONY
OF
JOSHUA A. CRISOSTOMO
POLICY ANALYST
NATIONAL SECURITY DIVISION
THE AMERICAN LEGION
BEFORE THE
HOUSE COMMITTEE ON HOMELAND SECURITY
ON
"WORLDWIDE THREATS TO THE HOMELAND"

DECEMBER 11, 2025

TESTIMONY
OF
JOSHUA A. CRISOSTOMO
POLICY ANALYST
NATIONAL SECURITY DIVISION
THE AMERICAN LEGION
BEFORE THE
HOUSE COMMITTEE ON HOMELAND SECURITY
ON
"WORLDWIDE THREATS TO THE HOMELAND"

December 11, 2025

Chairman Garbarino, Ranking Member Thompson, and distinguished members of this Committee, on behalf of National Commander Dan K. Wiley, and more than 1.5 million dues-paying members of The American Legion, we thank you for the opportunity to offer our statement for the record.

The American Legion is guided by active Legionnaires who dedicate their time and resources to serve veterans, service members, their families, and caregivers. As a resolution-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.

The American Legion thanks you and the members of this committee for your unwavering support for our nation's security. The American Legion believes the national security of the United States of America is of utmost importance amidst evolving threats.

Background and The American Legion's Relevant Work

The American Legion is a leading voice on national security, beginning with our advocacy for advancing military quality of life, maintaining the lethality of our armed forces, stronger border security, and fostering disaster preparedness in our communities.

National Security is one of The American Legion's four pillars, supported by resolutions dedicated to maintaining a strong national defense and safeguarding the nation. Comprised of Legionnaires, The American Legion's National Security Commission advocates for national security related issues. Under this Commission, the Law and Order and Homeland Security Committee reviews the objectives of the U.S. Department of Homeland Security and makes homeland security policy recommendations to the Administration and to Congress.

National Security Division Staff, in support of the Commission, has a history of identifying and recommending solutions to key homeland security issues which include cybersecurity threats and transnational criminal organizations.

Cybersecurity Threats

Cybersecurity threats continue to evolve in complexity and create vulnerabilities that could negatively impact all Americans. Cyber-attacks significantly threaten and impact civilian infrastructure, including essential services and commercial software. Historically, cyber-attacks originating from near-peer adversaries have targeted state and local governments and have directly affected food and water services, financial systems, and private companies. Local governments remain particularly vulnerable to these attacks, as they often lack the technological sophistication to protect their systems. These attacks put domestic infrastructure at risk, which could have deep impacts on American communities and local economies. Over the past year, several high-profile attacks have occurred against local, state, and federal levels of government, local communities, cities, and private companies.

In light of the constant threats, we urge Congress to swiftly exercise oversight measures to audit and improve security authorities in the wake of increasingly sophisticated cyber-attacks on our critical infrastructure and services. Due to the interwoven cyberspace of public and private entities, immediate action is necessary for the United States to maintain a resilient posture against an evolving cyberattack landscape. Additionally, inter-agency programs that promote public and private sector cyber-threat collaboration, as well as programs that grant cybersecurity funding to state, and local governments must continue to be prioritized and funded.

Cyber-Attacks

Earlier this year, the "Salt Typhoon" cyberattacks against American telecom companies, government entities, and a state Army National Guard network compromised telecom, infrastructure, and sensitive military network data.[1] This large-scale breach highlighted the vulnerability of interagency networks that support critical infrastructure services. As cyberattacks become increasingly sophisticated, cybersecurity is not solely a federal concern but a shared responsibility across government, industry, and the public.

The American Legion's Resolution No. 20: *National Cybersecurity Strategy*[2], highlights the need for greater interagency and commercial coordination to build cyber resilience through information sharing of best practices and standards.

The Space Domain and Cybersecurity

The cyber domain is interconnected with the space domain, as satellites are critical for enabling communications, data transfer, and GPS. These systems support critical infrastructure such as domestic energy and utilities, hospitals, the finance industry, telecommunications, and the aviation industry. As the space domain is increasingly an integral part of our lives, bad actors may exploit space-based system vulnerabilities to further their geopolitical gains. Throughout the Russia-Ukraine War, Russia has effectively damaged fundamental elements of space infrastructure through regular electronic attacks on communications satellites in space, demonstrating effective

[1] Office of Intelligence and Analysis, Department of Homeland Security. "Cyber Threats: Salt Typhoon: Data Theft Likely Signals Expanded Targeting." June 11, 2025. https://www.documentcloud.org/documents/25998809-20250611-dhs-salt-typhoon/ .

[2] The American Legion Archive. "Resolution No. 20 National Cybersecurity Strategy." August 24, 2017. https://archive.legion.org/node/532.

cyber capabilities against space-enabled communications.[3] These malicious attacks against space resources are likely to increase in frequency and intensity in the future as the effectiveness becomes more evident through impacts on intended targets.

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 military assets. 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 allies. This introduces a new kind of arms race into international cybersecurity.[4]

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 activities in space have also expanded with approximately 60 countries investing in new space capabilities, making space a crowded environment for policy. As a result, the risk of mismanagement has heightened. Thousands of satellites relying on overlapping frequency bands raise issues of signal interference and overall, degraded system performance.[5]

As the number and complexity of space actors grow, current U.S. governance structures are not keeping pace with this rapidly evolving landscape. The U.S. Defense Industrial Base (DIB) can counter these attacks in much the same way as with cyber-attacks; by increasing public-private partnerships strengthening strategic communication and expanding information sharing. 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 will 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.

The American Legion's Resolution No. 48: *Rebuilding the U.S. Defense Industrial Base,*[6] calls for revitalizing the DIB, reinforcing supply chains, modernizing production capacity, and investing in

---

[3] 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.

[4] "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.

[5] 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/.

[6] The American Legion Archive. "Resolution No. 48: Rebuilding the U.S. Defense Industrial Base." August 31, 2023. https://archive.legion.org/node/15097.

a skilled workforce. Without such investment, the U.S. risks compromising the ability to deter, respond to, and prevail in cyber conflicts.

Congress must address the domestic cybersecurity workforce shortage, as the need for skilled AI and cybersecurity professionals significantly exceeds the supply, leaving the U.S. vulnerable. Investing and expanding cybersecurity training programs and education are essential to the future of our homeland security.

Cybersecurity Threats from Global Adversaries

Over the past several years, Russia, China, North Korea, and Iran have been linked to increasingly sophisticated cyberattacks against the U.S. The Cybersecurity and Infrastructure Security Agency (CISA) published threat advisories warning against Iranian and Russia-state sponsored cyber threats over the past two years. In 2025, CISA detailed a threat from a Russia cyber campaign targeting American and other Western companies involved in the delivery of aid to Ukraine.[7] Earlier this year, North Korea evaded targeted U.S. private companies to illicitly generate revenue for its regime through mass infiltration efforts provided by remote-work opportunities.[8] Additionally, many of these North Korean actors involved in this fraudulent hiring practice used stolen identities and accessed sensitive employer information, U.S. military technology, and virtual currency.[9] As remote-work opportunities are a commonplace feature of the private sector, these incidents from North Korea provide a playbook for other state-backed organizations to emulate and generate illicit revenue from American citizens and companies.

Government agencies must aggressively protect Americans and businesses from being victimized by international illicit revenue generation schemes that undermine our national security and financial sector. Not only is interagency collaboration required to effectively combat these complex international cyber threats, but private industry information sharing is necessary to adapt against these evolving threats. Proactive outreach across private industry will provide a strengthened defense mechanism for businesses to patch known vulnerabilities in their operations.

Congress should continue to support and fund agency programs such as the DHS's Science and Technology Directorate and CISA to overcome global cyber-threats through collaboration with academia, industry, and government. CISA's active coordination with state and local governments enhances cybersecurity across the country.

Transnational Criminal Organizations (TCOs) Threats

[7] Cybersecurity and Infrastructure Security Agency. "Russian GRU Targeting Western Logistics Entities and Technology Companies." Cisa.gov. May 21, 2025. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a.

[8] Federal Bureau of Investigation. "North Korean IT Worker Threats to U.S. Businesses." Fbi.gov. Public Service Announcement. July 23, 2025. https://www.ic3.gov/PSA/2025/PSA250723-4.

[9] Department of Justice. "Justice Department Announces Coordinated, Nationwide Actions to Combat North Korean Remote Information Technology Workers' Illicit Revenue Generation Schemes." Doj.gov. Office of Public Affairs. June 30, 2025. https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote.

Transnational criminal organizations (TCOs) are one of the most dynamic and imperative threats to the homeland. They operate as multinational enterprises by trafficking drugs, weapons, humans, and laundering money across international borders with increased speed, sophistication, and boldness. Although their origins are primarily abroad, the impact of their activities is keenly felt in American neighborhoods through overdose deaths, violence in our communities, the exploitation of our vulnerable citizens, and the dismantling of legitimate commerce and financial networks.

The American Legion's Resolution No. 8: *Combatting Transnational Criminal Organizations (TCOs)*[10], advocates for the U.S. government to prioritize the elimination of transnational organized crime in all its forms. As TCOs operate without regard for borders, it is imperative for collaboration to occur with regional allies to secure our borders from illegal drug trade, human trafficking, and other criminal activities.

We urge Congress to elevate the threat posed by TCOs to national security priority status, with particular attention to homeland-relevant issues surrounding the synthetic drug crisis, illicit financial networks, and the important role of artificial intelligence in homeland security infrastructure. As authorized under the Immigration and Nationality Act, The American Legion supports the designation of TCOs as FTOs. Earlier this year, the Department of State designated multiple TCOs as foreign terrorist organizations (FTOs) and Specially Designated Global Terrorists (SDGTs).[11] Congress must evaluate whether these designations lead to reduced TCO criminal activity in the U.S.

Precursor Chemical Supply Chains and the Synthetic Drug Crisis

In 2024, fentanyl and other synthetic opioids were the most lethal drugs trafficked into the U.S., causing more than 52,000 U.S. deaths.[12] Unregulated Chinese chemical producers and criminal syndicates continue to be the major supplier of fentanyl precursors that find their way to Mexican cartels. The precursors are then processed into synthetic opioids and smuggled, resulting in over 60% of all overdose deaths in the U.S.[13] In the wake of the recent trade and economic agreement with President Xi Jinping of China and President Donald Trump, China agreed to halt the flow of precursor materials used to make fentanyl into the United States.[14] With this historic agreement, Congress must closely evaluate both the effectiveness of these export restrictions and its impact on fentanyl trafficking in the U.S.

---

[10] The American Legion Archive. "Resolution No. 8: Combatting Transnational Criminal Organizations." October 10, 2024. https://archive.legion.org/node/16296.

[11] Department of State. "Designation of International Cartels." Office of the Spokesperson. February 20, 2025. https://www.state.gov/designation-of-international-cartels.

[12] Director of National Intelligence. "Annual Threat Assessment of the U.S. Intelligence Community." Dni.gov. March 2025. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.

[13] U.S. Government Accountability Office. "Fentanyl Continues to Be the Leading Cause of Overdose Deaths. What's Being Done to Combat Trafficking into the United States?" September 5, 2025. https://www.gao.gov/blog/fentanyl-continues-be-leading-cause-overdose-deaths.-whats-being-done-combat-trafficking-united-states#:~:text=A%20hundred%20times%20more%20potent,That%27s%20about%2048%2C000%20people.

[14] Tang, Didi. "China announces restrictions on chemicals after deal with Trump on fentanyl tariffs." AP News. November 10, 2025. https://apnews.com/article/fentanyl-china-trump-tariffs-export-restrictions-dee0989539d866b04b129574e63b3635.

TCO Financial Networks and Illicit Finance Within U.S. Borders
Cartels and criminal syndicates are deeply rooted in international and domestic financial networks. They launder billions of dollars in real estate, shell companies, cryptocurrencies, and trade-based schemes.[15] These monetary flows undermine the integrity of U.S. markets and often occur in daylight hours, exploiting legal loopholes in markets like private investment and high-end real estate. Ultimately, this illicit financial network enables TCOs to operate and sustain their criminal activities in our country.

Congress must enhance financial intelligence capacity at the Financial Crimes Enforcement Network, DOJ, and Office of Foreign Assets Control. Investment is necessary to close regulatory gaps, especially in real estate and cryptocurrency industries, and bolster the technical infrastructure for tracking illicit finance flows.

Homeland Security Infrastructure and Artificial Intelligence (AI)
Evolving AI technology has the potential to enhance homeland security efforts through improved interdiction efforts at the border and improved investigation of TCO criminal activities. At the border, autonomous systems are deployed to provide alerts on potential threats and enable timely responses. AI models assist with assessing passenger and vehicle risks in real time, allowing CBP personnel to make informed decisions at ports of entry.[16] These examples of AI applications enhance DHS's border security operations through improved efficiency. To investigate TCO crime, DHS employs AI to identify victims and offenders through image and speech recognition. These AI investigative tools help generate investigative leads for effective enforcement actions against TCOs.[17]

AI has the capability to improve and expand information-sharing across law enforcement organizations nationwide. As these AI tools generate large amounts of intelligence data, it is imperative for efficient and secure data sharing across government agencies to occur in real time. This promotes timely, interoperable, and effective collaboration to convey intelligence threats in a useful context for law enforcement efforts across the state local levels.

The American Legion's *Resolution No. 9: Artificial Intelligence,*[18] advocates for the development of responsible AI use to enhance our national security. As AI technology constantly evolves, Congress should continue investing in expanding and employing innovative AI technology for homeland security efforts to counter TCO activity. Additionally, Congress must exercise close oversight over procurement processes to ensure that AI technology acquisition is streamlined for maximum effectiveness to support homeland security operations.

---

[15] Chainalysis. *Organized Crime Shows High Level of Professionalization, Low Level of Crypto Sophistication*. May 2, 2025. https://www.chainalysis.com/blog/organized-crime-crypto/
[16] McCord, Antoine, CIO, Department of Homeland Security. "Department of Homeland Security AI Strategy." Dhs.gov. September 2025. https://www.dhs.gov/sites/default/files/2025-09/25_0926_cio_dhs_ai_strategy_for_omb_m-25-21_508.pdf.
[17] Ibid.
[18] The American Legion Archive. "Resolution No. 9: Artificial Intelligence." May 9, 2024. https://archive.legion.org/node/15953.

Conclusion

Chairman Garbarino, Ranking Member Thompson, and distinguished members of the Committee, The American Legion thanks you for your leadership and for allowing us the opportunity to provide feedback on threats to the homeland.

In our increasingly digital world, protecting our homeland from state sponsored groups and transnational criminal organizations requires a proactive approach to strengthen our cybersecurity infrastructure, promote public and private collaboration, and leverage innovative AI technology. The vulnerability of our critical infrastructure, financial systems, private businesses, and global supply chains necessitates an integrated, whole-of-government approach.

Congress bears a vital responsibility for ensuring that our homeland is resilient against these threats through effective legislation, appropriations, and oversight. The American Legion calls for swift action to make our domestic institutions agile against evolving worldwide threats.

Questions concerning this testimony can be directed to Nick Ruf, Legislative Associate, at nruf@legion.org.