
# 2025 Public-Private Analytic Exchange Program Topics

**Evolving Domestic Threats to Data Center Infrastructure:** Data centers, the backbone of our digital world, face a range of complex threats. This topic can analyze the evolving nature of cyber and physical security threats to data centers and their infrastructure and assess the trends, techniques, and procedures of anti-data center extremists, their main grievances and fixations, past and future targets, the nexus between seemingly disparate groups, and how private and public sectors can better safeguard data centers. Special attention can be given to denoting future trends, especially in the context of artificial intelligence (AI). Additionally, this topic could seek to discuss collaborative efforts between the public and private sectors by exploring how governments, businesses, and data center operators can work together to enhance physical and cyber security. Protecting data centers ensures the stability of our interconnected world.

**Quantum Technology for Homeland Security:** Quantum technology, with its remarkable capabilities, has the potential to revolutionize homeland security. This topic may consider how this emerging technology can tackle critical challenges and enhance our security infrastructure while highlighting prospective threats. Quantum computing can perform complex calculations at unprecedented speeds, improving cryptographic methods, logistics, threat detection, and resource allocation. Quantum sensors, with their high precision, can detect nuclear, chemical, and biological threats, enhancing surveillance and early warning systems. Integrating quantum technology into homeland security poses technical and logistical challenges, including the need for specialized infrastructure and trained personnel. However, continued research and collaboration across government, academia, and industry can significantly strengthen national security, addressing both current and emerging threats. This topic can explore in-depth the benefits and challenges of integrating quantum technology into homeland security.

**Security Implications of Large-Scale Displacement:** Mass displacement, whether due to conflict, natural disasters, or other factors, reverberates across multiple domains, profoundly impacting security. This topic can employ a cross-disciplinary approach and assess the security implications of displacement. They encompass political, economic, social, and environmental dimensions, such as: infrastructure planning, resource allocation, border management, public health, social integration, security and law enforcement, international cooperation, disaster preparedness and response, and economic stability. Displacement has also contributed to new pressure on natural resources, such as food and water, which creates new challenges to consider. This topic might also look at how human migration and displacement might change in the future, and what implications have not yet been considered.

**Strategies to Track and Address Precursor Chemicals in Illicit Drug Manufacturing:** Illicit drug manufacturing poses a significant challenge to public health, safety, and security. This topic may explore the scope of and possible solutions for tracking and addressing the product flows, supply chains, and technologies involved in acquiring precursor chemicals used to manufacture illicit drugs such as methamphetamines and fentanyl. The issue of precursor chemicals necessitates more comprehensive domestic actions, and it extends beyond any single nation. This topic can investigate how enhancing regulatory frameworks, leveraging advanced tracking technologies, and fostering international collaboration can disrupt these chemical supply chains. Additionally, the topic may address the public health and safety impacts of illicit drug manufacturing with the goal of developing long-term solutions to adapt to emerging trends in the use of precursor chemicals.

**The Dangers of Unmanned Aircraft Systems (UAS):** UAS, often referred to as drones, have become more accessible and versatile, presenting both opportunities and risks. This topic can explore the rapidly changing technology and the availability of low-cost, more capable UAS that pose criminal, terrorist, privacy, and intelligence threats. As part of this effort, the team may assess advances in UAS technology and capabilities, the impact of low-cost UAS on accessibility and proliferation, the types of threats posed by UAS (e.g., surveillance, smuggling, physical attacks, etc.), the regulatory landscape governing UAS use, and security measures implemented by private and public sectors to mitigate threats. Most domestic critical infrastructure is owned and operated by private entities, while federal, state, local, tribal, and territorial entities are responsible for its protection. This topic can explore the role of public and private sector organizations in protecting critical infrastructure and ways to better coordinate and collaborate between them. This topic can consider highlighting case studies of past incidents involving UAS and critical infrastructure. Finally, this topic may provide insight into future challenges and solutions related to emerging UAS threats and vulnerabilities, ranging from policy recommendations to innovative solutions to counter UAS threats.

**The Role of Cyber Attacks in Modern Conflicts:** Cyber attacks have emerged as a potent tool in modern warfare, representing a considerable threat to the critical infrastructure and defense systems that secure and stabilize the nation through their disruptive nature and ability to generate secondary and tertiary effects on society’s ability to function. Cyber attacks target essential systems, such as communication networks, energy grids, financial institutions, and transportation. Organizations have the responsibility to secure their systems, especially those that contain sensitive information. The topic can seek to highlight best practices in identifying near-term cyber threats; developing and implementing protocols to mitigate potential attacks; and the use of various early detection and warning methods to prevent the loss of entire systems. Operations conducted prior and during attacks, conflicts, or invasions that lead to widespread disruption will also be considered. Cyber attacks transcend borders, blur traditional warfare lines, and demand proactive defense. Understanding their role in modern conflicts is essential for safeguarding critical systems and maintaining stability.