PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

2024

Public-Private Analytic Exchange Program Synopsis

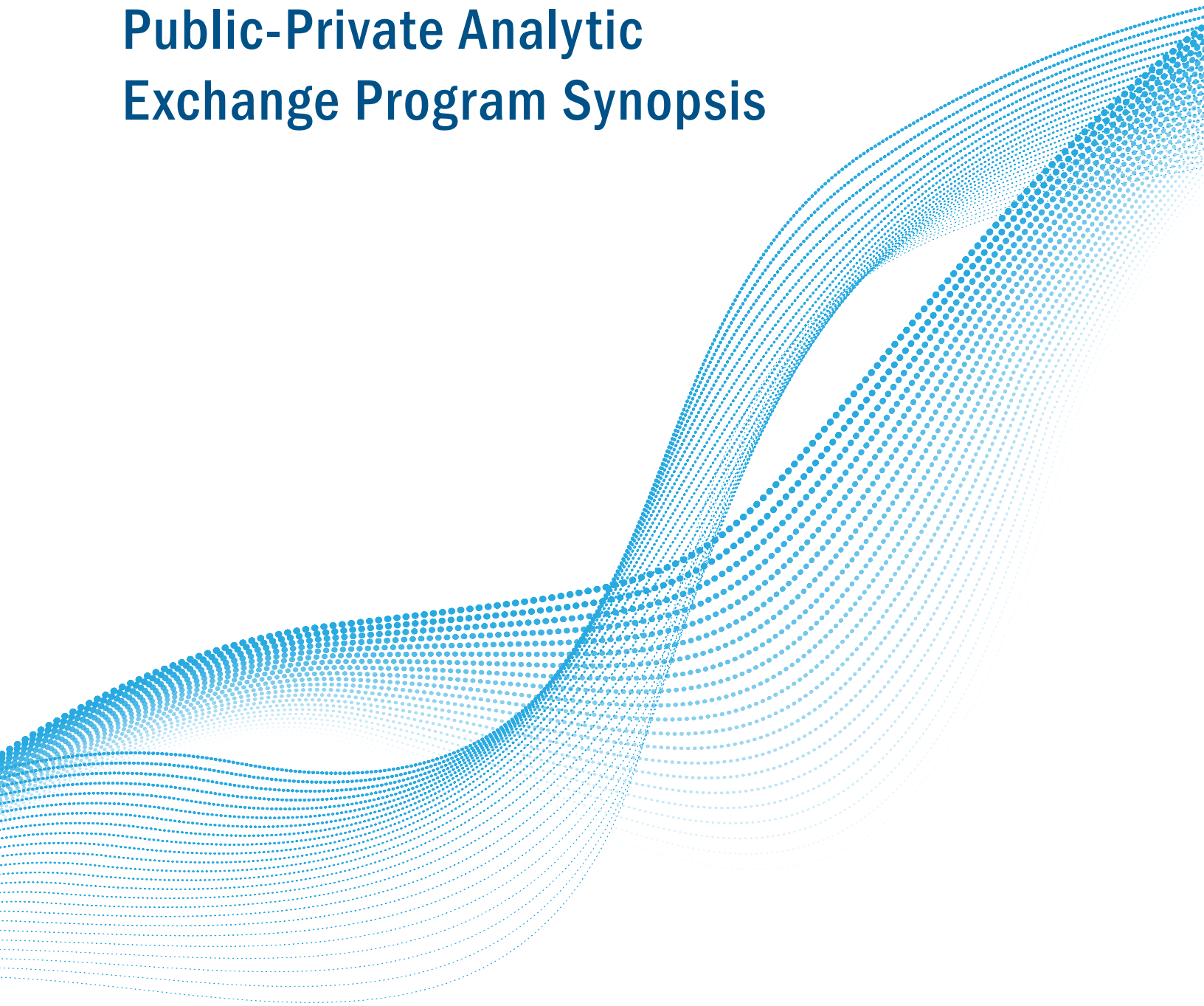


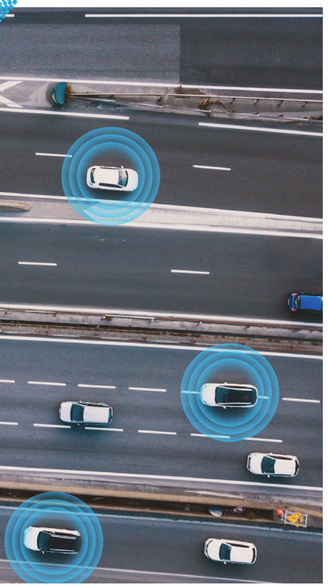
Table of Contents

Background

In today's dynamic and ever-evolving threat environment, it is important for both the public and private sectors to maintain situational awareness and actively coordinate and collaborate. By building partnerships and proactively sharing information, both sectors can increase their knowledge base and protect the people and companies within this great nation.

The Public-Private Analytic Exchange Program (AEP) is sponsored by the Department of Homeland Security's (DHS) Office of Intelligence and Analysis (I&A) on behalf of the Office of the Director of National Intelligence. DHS I&A facilitates collaborative partnerships between teams of government and private sector analysts to form several subcommittees to explore and increase mutual understanding of national and homeland security issues.

AEP Topic Team Abstracts



5G Impacts on Smart Cars and Highway Infrastructure Modernization

This team examined the impacts of 5G technology on vehicles and highway infrastructure, focusing on its transformative potential and associated cybersecurity challenges. The deployment of 5G technology is set to revolutionize vehicle automation and connectivity through faster data transmission, lower latency, and enhanced real-time communication between vehicles and infrastructure. These advancements promise significant improvements in traffic management, accident reduction, and overall user experiences. However, the increased connectivity also introduces new cybersecurity risks, necessitating robust security measures from the early stages of product development. The team identified key risk categories, including public safety, cybersecurity, and long-term sustainment, and emphasized the need for comprehensive strategies to address these challenges. They also highlighted the importance of public-private collaboration, standardization, and the federal government's possible role in facilitating the adoption of technical interoperability and cybersecurity standards to ensure safe and reliable operation of 5G-enabled transportation systems.

Assessing Risk in Multinational Investment Strategies

This team assessed the immediate needs of key stakeholders regarding improving Intelligence Community (IC) knowledge, tradecraft, and capabilities in assessing national security risks from foreign investments in the United States. In their due diligence involving both past and present stakeholders who focus on economic security issues, including supporting the Committee on Foreign Investment in the United States, they identified a definite need for formal training for these analysts to develop their knowledge of financial markets and the mergers and acquisitions (M&A) dealmaking process. To address this challenge, the team initiated the development of a specialized course that will train IC analysts and other relevant staff in learning fundamental concepts, ideas, and frameworks related to the structure and functioning of financial markets. Additionally, IC analysts and staff will learn how M&A deals are made, as well as relevant current topics with specific applications to economic security and screening foreign investments. Not only will this training further bolster familiarity for IC components who work in this increasingly important aspect of strategic competition, but it will support significantly enhanced private sector cooperation on these issues, which is a key aspect of protecting US national security.

Impact of Artificial Intelligence (AI) on Criminal and Illicit Activities

This team surveyed the state of generative artificial intelligence (AI) technologies as of mid-2024, examined the current and possible future criminal use cases for these technologies, and considered what mitigation strategies would be most effective in combating this threat vector. Generative AI refers to AI models that can produce realistic synthetic media such as images or text because they have been trained on vast amounts of data to learn the data's underlying structure and patterns. This team provides a conceptual overview of how generative AI works and summarize the types of generative AI models, including what they can do, their advantages, and their limitations. The 'Surveying the Criminal Misuse of Generative AI,' section of the team's paper discusses how this technology can make it easier or quicker to accomplish well-established crimes and how this technology creates opportunities for novel crimes. Critical to generative AI's applicability in the criminal space are its abilities to assist with coding, create content that looks legitimate, and quickly create large quantities of content. The final part of the paper outlines what the team assesses as high-impact mitigation strategies. This team found that existing mitigation efforts are often piecemeal due to this technology's fast-paced development and wide reach. Different expertise and capabilities are spread across numerous groups, and the paper presents an argument for strategic collaboration to enable information-sharing, stronger preventative measures, and action against criminal elements that use generative AI.

Impact of AI on Traditional Human Analysis

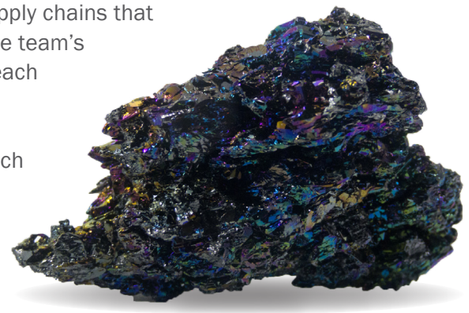
This team studied the rapid advancements in Artificial Intelligence (AI) technologies that are revolutionizing the way public and private organizations conduct traditional human-driven analysis, impacting all levels of the analytic design process. The team's report explores potential advantages and pitfalls that AI poses to each step of the intelligence cycle—from requirements and planning to collection, processing, analysis, production, and dissemination. The paper highlights the potential for AI to enhance efficiency, accuracy, and decision-making within all aspects of the intelligence cycle while also addressing ethical considerations and challenges.

Preventing Violent Extremism Tool Kit

This team conducted research and discovered an abundance of existing violent extremism prevention tool kits and programs. The threats of targeted violence and violent extremism have reached a critical inflection point with the recent assassination attempt of a former President of the United States. Fueled by the polarization of society, foreign conflicts, civil unrest, and the spread of disinformation, it is imperative to stop targeted violence and violent extremism before they spread. Given the complexity of prevention, no single program can address all the factors leading to violence. This team discovered that each instance requires different approaches depending on varying factors. Identifying and selecting the intervention best suited to the specific context of each community is crucial, as the drivers of violent extremism can vary significantly across different regions and populations. However, due to the vast number and complexity of available prevention programs, stakeholders are finding it more challenging to identify and implement the most suitable programs for their specific needs. To address this gap, this team proposes the development of the Violent Extremism Conceptual Comparative Tool of Resources, a platform that will help guide users to the program that best fits their circumstances. The tool will have users answer a few basic questions to identify their situation, resulting in a list of relevant tools and programs. This accelerated decision-making process would allow for earlier implementation of interventions, which is crucial in mitigating violent extremism.

Threat of Limited US Access to Critical Raw Materials

This team explored the implications for US industry's inability to obtain critical raw materials (CRMs). Despite some policy efforts by US government and private industry alliances, CRM shortages are projected to become one of the most critical challenges to the US economy, in part due to increasing demand, as well as an opportunity for foreign adversaries that exercise outsized control of CRM supply chains. This team identified major misalignments in US public-private sector approaches to CRM supply chains along with mitigation opportunities. The team also investigated foreign actor threats to the supply chains that could undermine US economic and political power. The team's methodology includes investigating misalignment at each stage of the life cycle of a CRM—discovery, mining, processing, manufacturing, sales/exports, recycling/end-of-life—and proposing potential mitigations. At each stage, the team examined the potential foreign actor threat and ranked their capability and intent. Their deliverable concludes with recommendations for the next stage of research.



US-China Competition: Tools of Power and Impacts

This team examined the nature, breadth, and implications of the People's Republic of China (PRC)'s influence efforts targeting US Homeland entities at the subnational level, such as with state and local government officials, university staff, and corporate executives. In performing their research, the team studied the broader context of the US and the PRC's roles and aspirations for the international order, and particularly the PRC's position as a challenger to existing US dominance. The team's research included a survey of existing open-source literature and reports, as well as interviews with subject matter experts on topics, such as the evolution of US-China relations, the PRC cyber threat, PRC influence within the US research community, and the PRC's methods of coercion among US businesses and the US-Chinese diaspora. The team's research was intended to inform US decision-makers operating at the subnational level on the range of influence activities they could face during interactions with PRC-linked entities, underscore factors to consider when weighing the overall risks associated with such interactions, and provide them with constructive options for mitigating the risks associated with PRC engagement—while emphasizing that not all social, cultural, and economic engagement with Chinese entities are malign or disadvantageous.

AEP Phase II Topic Team Abstracts

Originating in the 2023 AEP, these Topic Teams identified areas to explore further and requested to continue their research efforts from the previous year.

5G Impacts on Cybersecurity

This team conducted research on 5G ecosystems and technology environments for commercial cloud services. Their deliverable briefly explains 5G technology, its standards and potential benefits, and its concerns, along with a description of the standardization process driven by bodies such as Third-Party Product, Global System for Mobile Communication and International Telecommunication Union. The importance of addressing the implementation perspective of 5G in an evolving and complex cloud-environment is brought to the forefront by effectively addressing the challenges in cybersecurity, the futuristic impact of AI on 5G, along with sustainable solutions and mitigation measures such as the potential role of blockchain. Applications of 5G to the healthcare industry and how 5G can improve grid management are discussed in the context of innovation, economic growth, scalability, flexibility, speed, and connectivity. From the standpoint of standardization and security standards, the significance of utilizing specific strategies and technologies for securing 5G applications in power grid management is highlighted. The most important component of this research is the rapid evolution of the cloud environment and its implications on the evolution of the 5G Standalone Non-Public Network (SNPN). This research examines cloud-security guidance, as well as the implementation of detection and mitigation of risks to the evolving cloud environment. A cloud-centric threat informed guidance would keep pace with the rapidly changing cloud technology and services landscape. This deliverable also defines and explains the cloud environments supporting 5G SNPN and introduces the different types of cloud environments (public, private and hybrid), interactions between cloud, and cloud providers and security aspects of the cloud.

Implications of Extreme Weather Events

This team identified that the telecommunications sector provides vital services relied upon by nearly all individuals, businesses, and state and local governments. As a result, disruptions could have a debilitating impact on all 16 critical infrastructure sectors, hindering national security. Based on the research and results discovered during Phase I, the team identified consistent gaps concerning the cascading impacts of extreme weather on US fiber-optic telecommunications infrastructure, which facilitates the high-speed transmission of data enabling communications and supporting data-intensive applications. The team studied the unique threats posed to undersea cables, landing stations, the terrestrial cable network, and data centers, and identified several key questions that would best be answered by people with first-hand experience with extreme weather events. To gain deeper insights, this team ventured to New Orleans, LA—arguably the most challenging extreme weather environment for telecommunications infrastructure in the United States—to engage with various stakeholders, including an international telecommunications firm, a community-based organization, and federal and local government agencies. This research highlights industry best practices, such as continuous monitoring, redundancy, and disaster preparedness and planning. The findings emphasize the importance of service prioritization, siloing of localized knowledge, consideration of cascading impacts, supply chain disruptions and security, and a lack of centralized organization and oversight. Despite these challenges, the team noted an encouraging shift towards proactive and long-term adaptation strategies against extreme weather events.

US Maritime Trade and Port Cybersecurity

This team created a tabletop exercise that was used during site visits to showcase the development of the final executive presentation and accompanying assessment for port officials who are identifying the economic and supply chain considerations of cyberattacks against US port infrastructure. Aging information technology systems, veiled supply chain dynamics, the lack of a standard supply chain risk approach, social engineering attacks, and operational technology vulnerabilities offer attack surfaces that malicious cyber actors can exploit to disrupt port activities and cause irreparable economic harm on a national scale. The project builds off a Phase I effort, which identified vulnerabilities in port cybersecurity architecture and explored a range of legislative, policy, government, and private sector solutions to address the present risks. The deliverables aim to provide government and port officials actionable insights and recommendations to mitigate threats, enhance cybersecurity resilience, and minimize the economic and social impacts of successful attacks. Examples include setting minimum standards for infrastructure, proactively investigating upstream cyber supply chains, identifying best practices in incident response through contingency planning, exercises, and case studies, and improving information sharing within the port industry and across government.

AEP Phase III Topic Team Abstract

Originating in the 2022 AEP, this Topic Team identified areas to explore further and requested to continue their research efforts from the previous two years.

Combating Illicit Activity Utilizing Financial Technologies and Cryptocurrencies

This team continued examining the use of digital assets and their correlation to illicit activity, which has been rapidly developing over the past three years. In the previous two cycles of this program, the team sought to provide great research into the use of digital assets and emerging financial technologies in criminal activities, and how to effectively combat criminal activity in this space. This team decided to do a final phase to address some areas that were briefly referenced, but not fully addressed in the previous two cycles. These include central bank digital currencies, zero-knowledge proofs, AI influence on cyber-financial crimes, current/updated trends in the digital asset space, and recent rulings that have shaped the future of punishments for cyber-financial crimes. The key to combating criminal activity in the digital asset space and among emerging financial technologies is increasing awareness and informing stakeholders just how impactful it can be. The previous two AEP deliverables have done just that: increased awareness and shared information; however, the team always aims to reach a larger audience. This team seeks to continue arming colleagues, constituents, and general consumers with increased knowledge in this space.

Outcomes

The AEP is proud to highlight achievements made by current and former topic teams. The work of these teams has continued to stay relevant and provide insight for various partners.

» All deliverables are disseminated to over 25,000 recipients via the Homeland Security Information Network and are posted on the DHS public website at www.dhs.gov/aep-deliverables.

» In July 2024, the 2021–2024 Combating Illicit Activity Utilizing Financial Technologies and Cryptocurrencies topic team's research was included in an Emerging Technology Newsletter published by the DHS Office of Intelligence and Analysis.

» In November 2023, AEP participants were invited as guest speakers for a webinar hosted by the United Nations Population Fund (UNFPA) in collaboration with a doctoral research presentation by a fellow AEP participant. Officials joined from across the globe to learn more about the impact of the AEP deliverables in making all spaces safe. The webinar titled "Making All Spaces Safe" was hosted in New York at the headquarters of the UNFPA:

- The four AEP topic team deliverables presented were:
  - 2023: 5G Impacts on Cybersecurity
  - 2022: Increasing Threats of Deepfake Identities
  - 2018–2021: Vulnerabilities of Health Information Technology Systems
  - 2018–2019: Artificial Intelligence–Using Standards to Mitigate Risks

» In September 2023, the 2021 Threats to Food and Agricultural Resources topic team member was a part of a video presentation released by the North Carolina State University's Office of the Provost titled "Where Does Our Seafood Come From? Wicked Problems, Wolfpack Solutions." Some of the findings from this team's analytic deliverable was included in this video.

» In July 2023, the 2023 Implications of Extreme Weather Events topic team received a significant amount of interest in its Pharmaceutical Case Study given the recent shortages of antibiotics, heart medications, and cancer therapeutics. The White House Chief of Staff heard about their research and set-up a meeting for a team member to brief the Director and Deputy Director of the Domestic Policy Council. This led to additional briefings and information sharing of this study.

Notes

Notes

Notes

Notes

PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

For more information, please contact us at: AEP@hq.dhs.gov
To review AEP deliverables please visit: www.dhs.gov/aep-deliverables

September 2024
24-362-IA