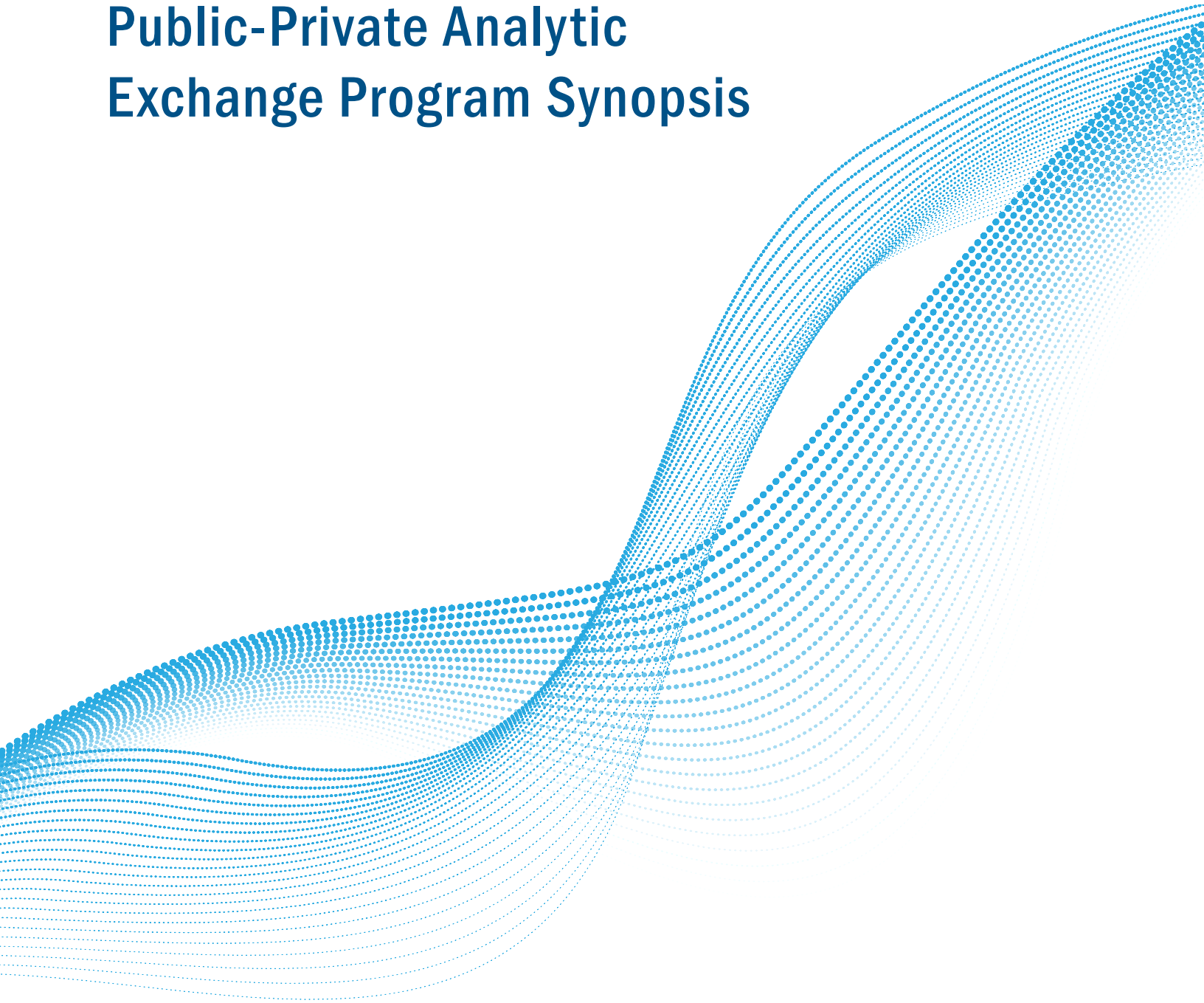
PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

2022

Public-Private Analytic Exchange Program Synopsis



PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

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 the public and private sectors can grow 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 (ODNI). DHS I&A facilitates collaborative partnerships between teams of experienced government and private sector analysts to form a number of teams to explore and mutually increase understanding of national security and homeland security issues.

Outcomes

Past outcomes beyond the AEP include:

- All deliverables are disseminated to over 25,000 recipients via the Homeland Security Information Network and are posted on the DHS and ODNI public website.
- I&A was contacted by the United Kingdom's Defense Science and Technology Laboratory (DSTL), which sought to gain a better understanding of AEP and its operating procedures. The UK's DSTL is planning to establish a program that replicates the AEP to encourage collaboration between government and industry.
- The "Vulnerabilities of Healthcare Information Technology Systems" topic team analytic deliverables, "Phishing Don't Be Phooled" and "A Lifeline: Patient Safety and Cybersecurity," were cited during the National Congress of the Italian Association of Clinical Engineers conference in Riccione, Italy.
- In 2022, the Central Bank of Ireland, Policy and Relations Security Division, reviewed the "Importance of Private Sector Intelligence Programs" 2021 topic team deliverable and requested the team's survey questions to assist with strategies to implement intelligence programs.
- In 2022, AEP deliverables were shared with the Hindustan Institute of Science and Technology as part of New York Medical College's empowerment programs in India. The university students found the deliverables very useful for their research projects, and an AEP alumnus has been invited as a guest speaker to discuss "health information in a digital world" and the most recent research findings in the field of science and technology.

2022 AEP Topic Team Abstracts

Addressing Risks From Non-State Actors' Use of Commercially Available Technologies

This team identified the risks associated with non-state actors' use of commercially available technologies deemed the most concerning by its own research team. The technologies included in this deliverable were based on real-world case examples, team members' professional experiences, and team research. The deliverable included, but was not limited to, technologies with past real-world examples affecting the Homeland, highlighting the likelihood of a non-state actor using each example and what the potential threat could be as the technologies become more capable and available to non-state actors.

While this deliverable will attempt to explain how various technologies pose risks to the US Government, critical infrastructure, and private sector partners, it does not provide an exhaustive list of all commercially available technologies used by non-state actors and addresses only those deemed most concerning by this AEP team.

Non-state actors have always been interested in obtaining and utilizing innovative emerging, advanced, or even simply commercially available technologies in support of tactical operations. Non-state actors—encompassing terrorist, insurgency, criminal, and lone actors—are not universally manned, trained, and equipped across the board. The accessibility of commercially emerging technologies is enabling more globally connected, resourceful, dynamic, well-funded, and technologically savvy non-state actors to level the playing field against better-equipped, nation-state actors. In previous decades, advanced technology was only in the hands of the few (military, corporations, academia) or a limited number of non-state actors compared to present day; individuals across the globe, including those in remote villages, are able to obtain and use technology such as smart phones. Additionally, new technologies have dramatically expanded threat actor groups' global reach, allowing these individuals to indoctrinate and recruit instantly via online propaganda at no cost and with relative anonymity anywhere in the world. Non-state actors also use a variety of commercially available platforms for fundraising schemes that have almost no boundaries for the exchange of goods and services. These non-state actors now have access to what once was military-grade technology. Many of the technologies that exist today are dual-use technologies that can be utilized for both civilian purposes and military goals.

Combating Illicit Activity Utilizing Financial Technologies and Cryptocurrencies

This team examined the use of financial technologies and cryptocurrencies by illicit actors. The key research points investigated include discovering the most common illicit finance activities, the most exploited elements of financial technologies, the legal vulnerabilities that allow exploitation, the pseudo-anonymity in online transactions, the weaknesses in Know-Your-Customer laws, and other emerging blockchain applications' (i.e., Non-Fungible Tokens) risk of use. The research gathered from investigating these areas led to the development of suggested, effective changes to reduce illicit activity in this space and helped identify key stakeholders to implement these changes. This paper seeks to provide guidance in navigating cryptocurrencies, emerging digital payments solutions, and other blockchain applications to both consumers and stakeholders to minimize the illicit use of these platforms. While illicit use will not be eliminated altogether, it can certainly be reduced with better consumer knowledge and enhanced practices/regulations issued by key stakeholders.

Countering Foreign Malign Social Network Manipulation in the Homeland

This team focused on the relationship between the public and private sectors as it pertains to countering foreign malign influence (FMI) on the Homeland. The team identified that a gap currently exists between the two sectors when it comes to specifically dealing with FMI. Through an interview process conducted over virtual meetings and email exchanges, private and public sector experts in the areas of public policy, trust and safety, and intelligence have provided valuable insights into the areas of misinformation, disinformation, and mal-information alongside the potential value of a public-private partnership on the issue of FMI. All answers and contributions are collated and presented anonymously by sector to ensure the safety, security, and privacy of those consulted for this project. The primary objective of this project is to develop recommendations for bridging the gap and to provide a model mechanism for partnership, information sharing, and tackling this challenge collaboratively.

Ethical Frameworks for Open Source Intelligence

This team conducted research on open source intelligence (OSINT), ethical frameworks, the history of OSINT, research tools, and the uses of OSINT. This paper covers these topics and provides a set of tools and guidance for how to apply OSINT ethics to everyday, online research. The objective of this paper is to better inform both the private and public sectors on ethical guidelines and how they relate to everyday, open source research. The misuse of open source data can be detrimental to any organization, person, and/or investigation the intelligence analyst may be performing. OSINT has become a very popular way to research a person, organization, or group, as it involves publicly available information. However, it is important for both organizations and researchers to follow ethical guidelines while researching and documenting public data. While organizations may not have a specific, ethical framework, it is important to keep research and information factual, sourced, and protected. Thus, this paper will help to provide OSINT researchers a framework to always keep an ethical mindset and high morals when researching subjects.

Evolving Landscape of US and Foreign Bioeconomy and Biotechnology

This team conducted research from the medical/healthcare field, defense/intelligence community, and corporate industry; the team also worked collectively to explore the current and near-term future of the biotechnology sector. This effort garnered reviews of national and international policy, the formative phase of defense critical infrastructure, medical supply chain vulnerabilities, and advancements in the biotechnology sector—specifically, how they may impact the US bioeconomy. The group decided that further exploration into the biological science field and the growing area of medical biological-convergence—or biomedical convergence (BMC), which synthesizes the biology and engineering fields—was necessary given the broadness of the topic. To further narrow the scope, the focus encompasses the application to enhance or extend human life as it relates to iterative and disruptive BMC technologies, the key role of data, and the concept of Human-as-a-Platform.

Given how intertwined the bioeconomy is with the economy at large, and the benefits advanced biotechnologies offer in enhancing and extending human life, there is a unique environment of competitive collaboration directly contributing to the safety, security, and wellbeing of mankind. However, the anticipated economic and national security implications within the biotechnology landscape will likely contribute to threats and vulnerabilities that the United States could be unprepared to manage on a societal scale.

The lack of international standards as it relates to bioethics, cybersecurity regulations, unregulated biomedical and biotechnology products, and processes with dual-use applications leads to challenges in the US national security and law enforcement landscape, which could have significant short- and long-term consequences for the United States and the global biotechnology ecosystem. This lack of international standards is heightened by outdated privacy and data protection standards, which allow for acute threats toward aspects of data analytics by way of artificial intelligence and machine learning (AI/ML).

Data science and AI/ML are expediting research in healthcare, mental health, and genetic engineering, supporting innovations that benefit human augmentation and the Human Platform Interface. Advances provide new ways to collect, synthesize, analyze, store, and use data. Understanding the (defense) applications and vulnerabilities that come with the advancements of biomedical research and development allows for planning and preparedness efforts should these technologies develop more rapidly among adversarial nations. Lastly, identifying the potential impact of the emerging BMC industry, and the data that surrounds the sector, is vital for a strong US security posture as the United States maintains a global leadership presence within the bioeconomy.

Increasing Resilience in Overlooked Critical Infrastructure Sectors

This team identified the chemical, food and agriculture, and water and wastewater systems sectors as having many elements associated with overlooked critical infrastructure and determined that these three sectors have an added variable that increases their vulnerability further: their interconnectedness with each other.

For example, the chemical sector supplies chlorine and sulfur dioxide for wastewater treatment in support of the water and wastewater sector and for pesticides, fertilizer, and consumable food additives used in the country's food and agriculture sector. Water and wastewater systems support the chemical and food and agriculture sectors by supplying large amounts of water for chemical manufacturing, industrial cooling, and farm irrigation.

In addition to depending on one another, the three sectors pose risks to each other as well. Pollution from chemical spills and agriculture runoff can harm the nation's freshwater supplies and increase the need for wastewater treatment. Interruptions in the supply of vital chemicals can endanger wastewater and agriculture operations, and water shortages or inadequate wastewater treatment can endanger chemical sector and agriculture operations.

Informed by interviews with industry experts from all three overlooked sectors, the team designed as its final deliverable a tabletop exercise and an accompanying exercise manual to raise awareness of the interconnectedness among the chemical, food and agriculture, and water and wastewater systems sectors with government and industry participants and stimulate discussion about how the sectors can work together to increase their resilience against shared threats. The exercise will be based on containing an insider threat scenario in one of the sectors and minimizing spillover effects on the other two sectors through engagement and collaboration with government and industry partners.

The tabletop exercise's objectives are to:

- Identify areas of dependency among the chemical, food and agriculture, and water and wastewater systems sectors that may impact owners/operators of critical infrastructure assets;
- Assess how an organization's emergency operations plan identifies and plans for functional dependencies outside the control of the critical infrastructure owner/operator;
- Identify critical entities across the chemical, food and agriculture, and water and wastewater systems sectors to serve as preparedness and response partners; and
- Share resources and best practices among critical infrastructure owners/operators on increasing resilience in recognition of dependencies across sectors.

Ransomware Attacks on Critical Infrastructure Sectors

This team identified that ransomware attacks against US critical infrastructure entities have increased significantly over the last several years, as defined by the Cybersecurity and Infrastructure Security Agency (CISA) and have become a national security concern. Most notably, in 2021, several high-impact cyber-attacks affecting critical infrastructure resulted in the widespread disruption of US fuel distribution, food processing, and corporate operations, spurring significant private sector and government efforts to counter ransomware and improve the cybersecurity of critical infrastructure owners and providers. Such efforts include sanctions targeting ransomware cash-out operations, the adoption of recommendations made by the Institute for Security and Technology Ransomware Task Force, and the Department of Justice giving ransomware investigations the same high priority as those involving terrorism. However, while the federal government has emphasized ransomware as a priority, we note concerns that the high number of government priorities has possibly hampered related efforts. One such example is that the Financial Crimes Enforcement Network's anti-money laundering priorities, which could help direct financial intermediaries to identify and report ransom payments, has yet to be fully incorporated into ongoing efforts. CISA estimated that, as of July 2021, only about one quarter of ransomware incidents were reported, which further highlights how many attacks have probably adversely affected critical infrastructure owners and operators in the United States.

This problem will be addressed by a white paper and a brochure. The white paper will discuss two key issues regarding the ability to combat the ransomware threat. The first issue is the current cyber threat environment and ways in which the US Government and its partners can deploy more effective measures to reduce the risk of ransomware attacks against private, public, and government entities that provide US critical infrastructure services. The second issue is the financial aspects surrounding ransom payments by victims, including economic intermediaries and the conversion of cryptocurrency into fiat currency. The paper will also document efforts to combat cyber threats and present possible improvements for US Government coordination and communications to mitigate ransomware attacks against US critical infrastructure. It describes the financial ecosystem that enables ransom payments, which includes victim dollars in bank accounts, ransom intermediaries, on-chain cryptocurrency, foreign currency, and cybercriminals. The paper will also have recommendations on how to disrupt the financial ransomware business model. Lastly, the paper analyzes government counter-ransom payment actions and evaluates the true cost caused by ransomware attacks on critical infrastructure. The brochure-style product is intended to educate public and private critical infrastructure owners and operators by identifying important useful and available resources, as well as educating financial institutions about their regulatory obligations regarding ransomware-related payments.

Threats to US Physical Trade & Supply Chain Integrity

This team examined existing and emerging physical and cyber vulnerabilities in our nation's maritime, air, rail, and trucking systems; analyzes the challenges and opportunities presented by those vulnerabilities; and proposes ways in which the public and private sectors can collaborate in a coordinated response to mitigate the risks posed by these vulnerabilities and enhance the resilience of our nation's supply chain. Weaknesses in the global supply chain were revealed by the COVID-19 pandemic and exacerbated by geopolitical events—including the war in Ukraine, the ongoing conflict in the Middle East, and the risk of war in the Far East—hold major national security implications for the United States.

2022 AEP Phase II Topic Team Abstracts

Originating prior to AEP 2022, these topic teams identified areas to further explore and requested to continue their research efforts.

Phase II: Importance of Private Sector Intelligence Programs

This team assessed research efforts from 2021, examining how government and corporate intelligence programs add vital capabilities to their parent organization's overall security effort. The team's research, which consisted of a literature review and survey of experts in the field, determined how such intelligence programs are commonly structured and operated, the perceived benefits and challenges of using them, and some recommendations to improve the sharing of information.

In Phase II, the team performed a deep-dive exploration of the actions corporate planners typically take when initially setting up intelligence programs within their organization. In

conducting its research, the team examined existing corporate intelligence concepts, a diversity of viewpoints among members of the group, and interviews with experts in the corporate security world.

The team's Phase II deliverable is a graphic representation of a model highlighting six key factors that must be addressed when establishing corporate intelligence programs to maximize the chances for a successful return on investment. Further, upon presenting its findings, the team highlighted ways in which incorporating this six-factor model has proven valuable when operating during the unique challenges of 2020–2021.

Phase II: Increasing Threats of Deepfake Identities

This team continued examining previous findings from the 2021 AEP Phase I of research and in-depth suggestions for organizational, legislative, and regulatory approaches to combat the impending threat of deepfake identities in three use cases. Deepfakes are a type of synthetic media—commonly generated using AI/ML—presenting plausible and realistic videos, pictures, audio, or text of events that never happened. The first use case addresses content offered by creators, owners, and immediate users like media organizations, nongovernment organizations, law enforcement, and legal institutions that rely on this content. The second use case addresses content associated with real-time or live scenarios for identity proofing and verification to enable and offer services and products; the real-time or near-real-time nature of the interaction in these scenarios make imagery, video, and audio content of particular importance. The third use case addresses content disseminated in the broadcast environment, where social media platforms and news organizations may be used as vehicles to disseminate false, misleading, and ultimately harmful information with broad impacts of varying magnitude. For each of these use cases, we determined the primary stakeholders who have an interest in identifying and implementing deepfake countermeasures. We isolated the main use cases and studied the threats associated with each use case, analyzing the policy, education, and technology actions that may help mitigate the risks posed by deepfakes.

PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

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

AUGUST 2022

22-328-IA