PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

2023

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 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's) 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 US government and private sector analysts to form several subcommittees to explore and increase mutual understanding of national security and homeland security issues.

2023 AEP Topic Team Abstracts

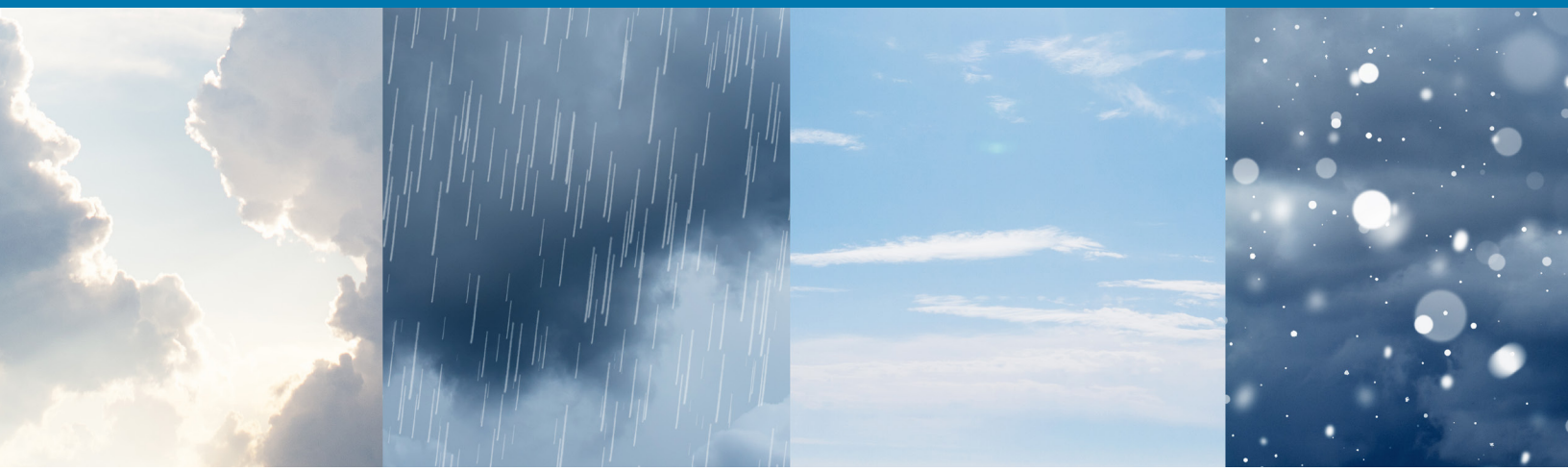
5G Impacts on Cybersecurity

This team conducted research on security issues related to the introduction of 5G mobile communications into the United States and abroad. The topic of 5G has been subject to a certain degree of hype, mischaracterization, and misunderstanding. These mischaracterizations, and the obstacles they present to understanding the 5G world and its security implications, inspired the team to take a survey approach to the 5G issue and contextualize the matter. The paper begins with an overview of the 5G ecosystem as it is developing and how it will mature. For the purposes of the 5G paper, it is better described as a fifth-generation wave of investment in mobile technology. Beyond that, the paper looks at threats to 5G technology and 5G networks; these threats are primarily technical in nature. The next section looks at threats coming from the adoption of 5G technology. The team looked at broader threat implications related to 5G, such as social and political implications of the emergent 5G environment; this includes issues related to human rights. These are threats that have not been as widely discussed as the more traditional technical threats. Having established a baseline description of the 5G ecosystem and the threats it imposes, the team looked briefly at the international aspects of these issues and their regulatory and policy aspects.

Chinese Counterfeit Microelectronics

This team focused on understanding the threats posed by Chinese counterfeit microelectronics, how they can be mitigated, and what resources are available to companies responsible for procuring and incorporating microelectronics in their products. The main focus of this product is to familiarize small- and medium-sized businesses involved in the business-to-business microelectronics marketplace with the potential risks of counterfeit acquisitions and ways to minimize those risks by mitigating their introduction into the supply chain.

Additionally, the team focused on the Chinese entrepreneur and commercial side of counterfeiting and smuggling, and determining why China has been the main source of counterfeiting to the United States. The team identified gaps that currently exist in the supply chain, as well as potential remediation efforts for those gaps. The team also traveled across the country to meet with government and private industry partners and experts for research. Through multiple interviews with industry leaders in both public and private sectors, the team helped to provide recommendations on protecting against counterfeits and enforce their industry trademarks.



Implications of Extreme Weather Events

This team noticed that the United States and the rest of the world are contending with increasingly common extreme weather events that threaten US national security. These extreme weather events have significant primary and secondary effects on the full range of critical infrastructure sectors and their supply chains—many of which enable key US government functions or support American society. This report examines public-private practices and methodologies to address the current and evolving threats to national security from extreme weather events. The analysis focuses on best practices and frameworks to be developed or updated by 2035 to address extreme weather threats out to 2050. The team began this analysis with an overview of the threat landscape to identify the types of extreme weather threatening the United States and the rest of the world, as well as the expected trends across each event type in the coming decades. The report assesses the national security implications of these weather events and how extreme weather events intensify existing threats or degrade the ability of the US government and the private sector from performing critical functions. The team highlights the importance of public-private cooperation to address the threat of extreme weather events through two case studies included in this report. The first case study examines the impacts of Hurricane Maria on the pharmaceutical industry's supply chains and the steps pharmaceutical companies have taken to build resilience. The second case study analyzes steps taken by the semiconductor industry in Taiwan to address a drought in 2021, which challenged manufacturing and threatened the global supply of microchips. The report provides mitigation options tied to specific extreme weather events and public-private best practices observed from the case studies and interviews with government and industry leaders. The report aims to give public and private sector stakeholders actionable steps they can implement in their organizations to build resilience and mitigate the impact of extreme weather events on national security.

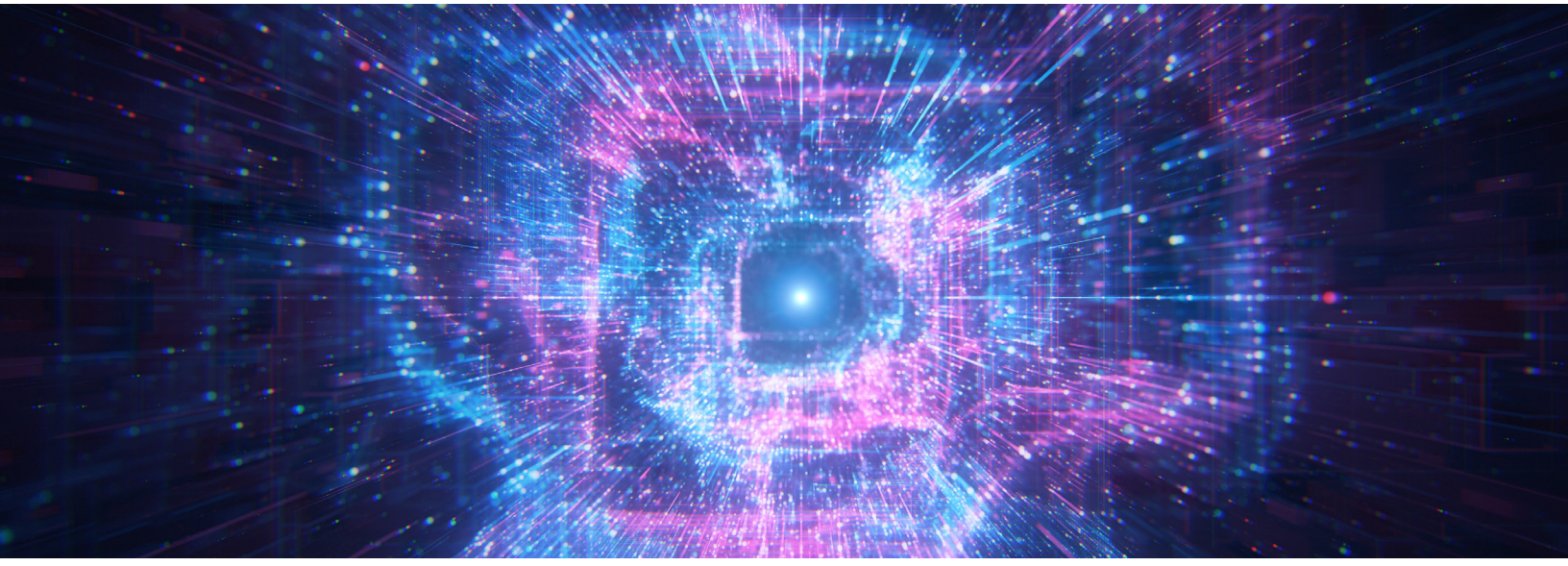
To ensure the widest use of this research, the Environmental Systems Research Institute (ESRI) platform will hold interactive datasets connecting current weather research, modeled forecasts in shifts for each extreme weather event trigger, thresholds for potential impact, and the case studies to focus data pertinent to each region, sector, and national security implication key concept of concern. The platform allows for display maps that pull the most up-to-date graphics, enabling this product to self-update and produce consolidated summary pages as new models and studies debut. The ESRI product will be maintained by DHS and updated as more tools, resources, and funding opportunities become available, making this product a living document and a collaborative effort.

National Security Readiness

This team's research was based on the idea that in today's increasingly complex threat landscape, our national security readiness will be better postured through increased public and private sector communication and coordination, especially with incidents impacting critical infrastructure. They reviewed over 70 after-action reports from exercises and real-world incidents nationwide impacting critical infrastructure between 2008 and 2022, which demonstrated the loss of communications as a critical issue and highlighted the need for redundant interoperable communications capabilities. In addition, a series of interviews and surveys with both public and private sector individuals showed a general consensus that, while communication coordination between the two sectors is not always strong, it was nevertheless a desired path for future development and security planning. The team's recommendations are informed by a literature review, analysis of after-action reports, interviews with stakeholders, and a nationwide cross-industry survey.

Rapidly Evolving Sanctions

This team examined the role of the People's Republic of China (PRC)—the world's leading supplier of Rare Earth Elements (REE)—and the potential implications of economically restrictive measures for the US government and US businesses with respect to market disruptions. The REE sector is a highly valued commodity industry and remains sensitive to supply chain disruptions. REE are critical parts of US and Western supply chains in the high-tech, energy, aerospace, defense, and healthcare fields, among others. The team explored how varying tensions impacting industries dependent on REE would evolve through four alternative analysis scenarios that focus on the risks and potential implications of changing geopolitical tensions. They found that in one extreme, US government and US businesses are preparing for the escalatory nature of economic conflict with the PRC despite the potentially severe negative economic implications for the global economy. The team also found that even in the best-case scenario, where political and economic tensions subside, the global economy will not revert to the level of economic efficiency enjoyed before the Trump Administration's trade restrictions on China in 2018.



United States Maritime Trade and Port Cybersecurity

This team examined the current threat landscape, challenges, and mitigations affecting the maritime trade and port sector. In an increasingly connected world, the security of our ports is paramount. The interconnected network of third-party vendors and foreign acquisitions of US port infrastructure present significant vulnerabilities for US port authorities. While significant advances have occurred in recent years, more improvement is needed to ensure that this sector is adequately protected from current and future threats. Vulnerabilities, whether old or new, must be addressed before cyber adversaries have the chance to compromise critical systems and assets within ports.

In this report, the team examined challenges to US port facilities from foreign investment and application programming interfaces. Maritime ports, facilities, and infrastructure worldwide are vulnerable to physical and cybersecurity exposure through foreign adversarial access to port equipment and supply chain information management systems. Specifically, proprietary foreign adversarial companies manufacture, install, and maintain port equipment that pose potential vulnerabilities to global maritime infrastructure information technology and operational technology systems. Utilizing a case study related to the issue of foreign cranes in US ports, the team highlights challenges, vulnerabilities, and recommended courses of action regarding how to mitigate potential vulnerabilities introduced by foreign investment in US ports.

Port community systems enable the exchange of information between private and public organizations operating within the port environment, increasing efficiency, and promoting ease of business—but also introducing vulnerabilities to the system. Unauthorized access to port community systems would likely enable adversaries to collect large sets of data on the US supply chain and the ability to delay/disrupt the maritime transportation system. Port community systems offer unique services tailored to best support the operations conducted at a port facility. Common services include terminal control, container status reporting, and scheduling/booking requests and confirmations. Using a case study related to the issue of vulnerabilities introduced through improperly configured scheduling systems and interfaces, the team highlights challenges, vulnerabilities, and recommended courses of action regarding how port facilities can better secure access points to their networks.

2022 AEP Phase II Topic Team Abstracts

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

Phase II: Addressing Risks from Non-State Actors' Use of Commercially Available Technologies

This team worked to address the risks posed by non-state actors' use of commercially available technologies. Technologies of particular concern include fast-growing artificial intelligence (AI), digital platforms, unmanned systems, and additive manufacturing (aka 3D printing). Non-state actors are using these technologies at an increasing rate and countering illicit use of these technologies requires a multi-faceted approach and public-private cooperation.

This deliverable describes current public and private efforts to address the risks and possible ways to overcome challenges stemming from new technology developments being adopted by non-state actors. It also discusses methods of risk mitigation, including legislation, policies, regulations, end-user agreements, awareness campaigns, and public education.

Phase II: Combating Illicit Activity Utilizing Financial Technologies and Cryptocurrencies

This team, comprised of private and public sector professionals and subject matter experts working in the cyber financial landscape, examined the use of financial technologies and cryptocurrencies by illicit actors. Phase I of this research focused on a general overview of the emerging illicit activity pertaining to digital assets and the peer-to-peer payment space. This included discovering the most common illicit finance activities, the most exploited elements of financial technologies, the legal vulnerabilities that allow exploitation, pseudo-anonymity in online transactions, weaknesses in Know-Your-Customer laws, and the risks of other emerging blockchain applications (i.e., non-fungible tokens). Phase II serves to build upon the foundation laid out in Phase I, with increased research into the criminal groups utilizing digital assets in illegal activities, how these criminal groups are conducting illicit activity/recruiting members, cryptocurrency ATMs/Point-of-Sales use, generative AI use in cybercrime, darknet market use of digital assets, the evolving use of cryptocurrencies (especially the year-to-date change), impacts on the government and private sectors, and additional policy recommendations. Although illicit use cannot be eliminated completely, it can be reduced with increased consumer knowledge, proactive law enforcement investigations, and better practices/regulations issued by key stakeholders.

Phase II: Generative Artificial Intelligence and Foreign Malign Influence

This team examined the near- and long-term threats and opportunities of generative artificial intelligence (GAI), current unknowns about this technology, and opportunities that governments and civil society may employ to better regulate and govern its deployment. The deployment and adoption of Large Language Models—including Chat Generative Pre-trained Transformer since November 2022—is a watershed moment for society. However, GAI also presents significant risks and opportunities for the US with its ability to create realistic and compelling content, including text, images, and audio, that could be used by foreign adversaries for malign influence. The ability of GAI tools to synthesize vast quantities of data, generate human-like text, and produce multilingual translations could augment human cognition, creativity, and productivity in the near term. At the same time, GAI, with its synthetic voice and audio capabilities, widespread availability, and low cost, effectively democratizes disinformation and could erode societal trust and expertise.

Phase II: Ethical Frameworks for Open-Source Intelligence (OSINT)

This team built upon its Phase I efforts from 2022, when they reviewed traditional ethical frameworks, the history of OSINT, OSINT tools, and the uses of OSINT in the public and private sectors. The team published a white paper after performing research and interviewing subject matter experts in the field. In Phase II, the team engaged in a more detailed look at OSINT Frameworks, focusing specifically on how companies impart ethics into their OSINT research. The Ethical Frameworks in OSINT team traveled to San Antonio, Texas, to meet with multiple private and public organizations to glean their insights on their security priorities and the role of ethics in their research. The participants also held multiple virtual interviews with subject matter experts from the private sector to gain knowledge on their OSINT processes. The Phase II Ethical Frameworks team operationalized its Phases I and II research by creating a "Scorecard" highlighting five key principles that companies can use to guide their OSINT research activities: 1) Furthers Mission and Reflects Core Values; 2) Respects Liberty, Civil Rights, and Other Protections; 3) Accurate, Timely, and Customer-Oriented Analysis; 4) Retention and Audit SOP; and 5) Empathy and Respect in All Actions. Each principle on the Scorecard is partnered with multiple questions, which are part of a self-grading system that provides companies with an in-house method of measuring progress toward establishing ethical OSINT processes. The Scorecard also includes Appendices that detail further resources and themes associated with ethical OSINT activities.

Outcomes

Past outcomes of the AEP include:

- All deliverables are disseminated to over 25,000 recipients via the Homeland Security Information Network and are posted on the DHS public website.
- Two AEP 2023 private sector participants were invited by the Defense Intelligence Agency (DIA) to partake as panelists in its Annual Defense Countering Terrorism Intelligence Conference and discuss violent extremist organizations with a variety of Department of Defense, US Government, and international partner organizations. Over the past several years, DIA has selected AEP Topic Team participants as speakers or panelists.
- The Combating Illicit Activity Utilizing Financial Technologies and Cryptocurrencies team presented its 2022 findings and 2023 initial findings at the National Cyber-Forensics and Training Alliance (NCFTA) conference. The NCFTA annually hosts this unique, invite-only conference that complements the cyber threat information sharing, miscreant hunting, and trusted public-private collaborative environment. This team was fortunate to participate and receive input and feedback from industry experts who provided valuable insights for its 2023 analytic deliverable.
- Three AEP deliverables ("Protecting and Defending Hidden Treasures," "Patient Safety and Cybersecurity: A Lifeline," and "Phishing! Don't be Phooled") were highlighted in a full-day cybersecurity workshop during the Healthcare Information and Management Systems Society Asia-Pacific conference in Bali, Indonesia. There were approximately 100 attendees from various regions of the Asia-Pacific region, including individuals from Indonesia, Malaysia, Enterprise Singapore, the Ministry of Health of Singapore, and Dell Technologies.
- A Defense Intelligence Agency officer commented that the *"AEP 2019 Counterterrorism Futures team's UNCLASSIFIED report is still relevant today. Their report on "Counterterrorism Futures and a Whole of Society Approach" was a forward leading and illuminating project that not only outlined potential terrorist threats and scenarios, but also drove home the critical importance of a Whole of Society examination of the threat. Furthermore, it provided critical space for conversations on how threats could be mitigated or dealt with from the private sector program. This concept is not only a key tool for the various US plans, policies, and strategies but also for our international partners. As the report is "UNCLASSIFIED", it gave our international partners a template, again not only what the threat may look like, particularly as it pertains to terrorist exploitation of evolving technology, but also on the centrality of the partnership with private sector elements on defining and dealing with these threats."*

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 2023
23-297-IA