2019 Public-Private Analytic Exchange Program Synopsis

PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

Background

In today's dynamic and ever-evolving threat environment, it is not only important for both the public and private sectors to both maintain situational awareness and actively coordinate and collaborate. Through building partnerships and proactively sharing information, we can grow our knowledge base and protect the people and companies within our great nation.

The Public-Private Analytic Exchange Program (AEP), 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), facilitates collaborative partnerships between members of the private sector and teams of experienced U.S. government analysts to form a number of subcommittees. This annual program provides U.S. government analysts and private sector partners a better understanding of select national security and homeland security issues.

Outcomes

Past outcomes beyond the Public-Private AEP include:

- All deliverables are disseminated to over 10,000 recipients via the Homeland Security Information Network and are posted on the Federal Bureau of Investigation (FBI) public web page.
- In 2019, the Transportation Security Administration (TSA) shared the 2017 Aviation Insider Threat team's deliverables with the Charlotte Douglas International Airport which plans to roll out the AEP's team pamphlets and posters on increasing insider threat awareness soon.
- Over the past two years (2018-2019) the Defense Intelligence Agency/Annual Defense Combating Terrorism Intelligence Conference has selected AEP topic teams to participate as speakers or panelists to share in discussions with a variety of Department of Defense, United States Government, and international partner organizations on violent extremist organizations (VEOs) and key functions VEOs rely on.
- The 2018 Artificial Intelligence team partnered with the Harvard Medical School to help facilitate collaboration with the Indian Government to launch the team's medical AI diagnostic tool to screen Tuberculosis on a national level in India. The Artificial Intelligence team also met with the director of the United Nations Program on HIV/AIDS (UNAIDS) and in 2019 one of the members of the team delivered a speech on "AI in Public Health" at a UNAIDS internal meeting.
- The 2017 Digital Blackmail team was selected to present findings at the International Association of Emergency Manager's 65th Annual Conference & Emergency Exercise in Long Beach, CA.
- The 2014 Unmanned Aircraft Systems (UAS) team published a white paper entitled "Unmanned Aircraft Systems: Security and Regulatory Challenges in U.S. Domestic Airspace" which addressed the challenges presented by the expected growth of domestic UAS operations for commercial and personal use.

2019 AEP Topic Abstracts

Best Practices in Vetting Prospective and Current Employees

This team examined how a variety of organizations across multiple sectors utilize screening procedures to hire and retain the right people for the right positions. The team developed a key intelligence question and operational definitions of key terms to assure standardized data collection processes. They utilized multiple data collection platforms, to include on-site and telephone interviews, and email surveys. Data revealed how, when, and why personnel are vetted for employment, and took into consideration how to evaluate insider threats and the cost vs. efficiency of the procedures.

The team found key takeaways to determine innovative concepts and successful implementation of tradecraft, techniques, and procedures for vetting of personnel. The identified procedures are not always applicable to all sectors and/or business sizes, but several emerged from the data, to include:

- Gauging buy-in to the organization's mission and strategic goals,
- Utilizing technology for background checks to ensure they are applicant-friendly and timely, and
- Conducting periodic checks for job fit, satisfaction, and to identify training that can keep the employee engaged.

Combatting Targeted Disinformation Campaigns

This team examined the social, political, technological, and policy challenges inherent in mitigating targeted disinformation campaigns. The team accomplished this through analysis of the current literature on the topic and through discussion with experts across the United States, which included on-site visits to Washington, D.C. and to the San Francisco Bay area. Consulted experts provided valuable information on the fundamental characteristics of disinformation campaigns and on the challenges in industry, society, and the regulatory/legal environment that hinder mitigation efforts.

The team's deliverable uses case examples to illustrate how disinformation campaigns work, who conducts them, and their impact on targeted audiences. The deliverable focuses on assessing common disinformation methodologies rather than concentrating on a specific threat actor. The goal is to identify key enablers common across disinformation campaigns, inform the public, and provide recommendations to government and private sector audiences to combat these campaigns and raise societal awareness and build resilience.

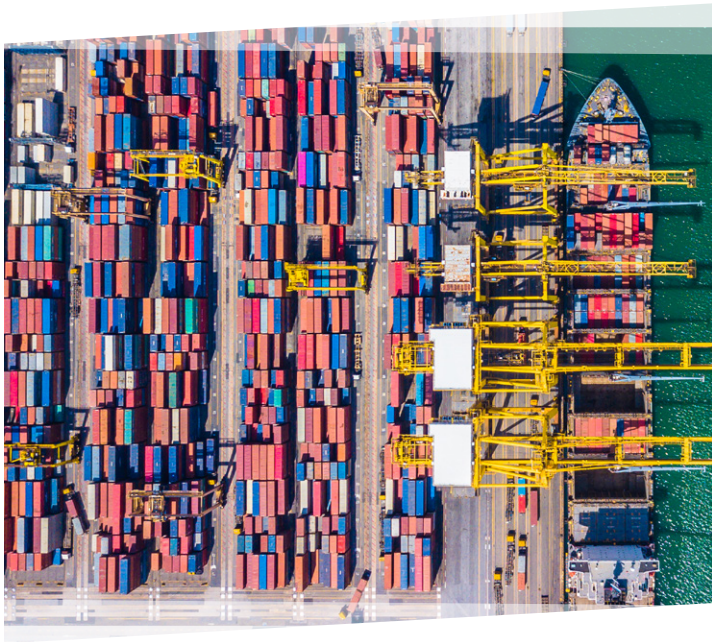
Counterterrorism Futures

This team assessed that in the next five years, the trend toward political and societal polarization will likely shape the domestic landscape, creating heightened levels of civil unrest and a more disperse extremist network, thus complicating the terrorist threat picture. This deliverable seeks to identify potential terrorist threats, including their use of non-traditional funding mechanisms (and use of new technologies) against nontraditional targets.

The team's deliverable discusses three case studies using near-term trends to identify exploitable vulnerabilities and suggests opportunities for enhanced public-private cooperation to address those vulnerabilities. The final section of the deliverable provides an expanded look into these partnerships and discusses a variety of information-sharing models that could strengthen public-private partnerships in ways that would sustain future counterterrorism initiatives, even in the face of declining public resources.

E-Commerce: Illicit Actors' Use of Reshipping Services

This team conducted a multi-month study to understand how illicit actors are exploiting their access to millions of commercial goods via electronic commerce (e-commerce) platforms in the U.S., as well as to understand their use of shipping services to move illicitly acquired goods. The data was obtained from interviews of US government officials and private corporations operating in the US, as well as open source research which included research on the dark web.



The team identified challenges faced by financial institutions, retailers, shipping companies, and the US Government in detecting, deterring, and mitigating this type of fraud. Based on research and analysis, the team will provide the private and public sectors with recommendations to combat and disrupt e-commerce and reshipping fraud in the future.

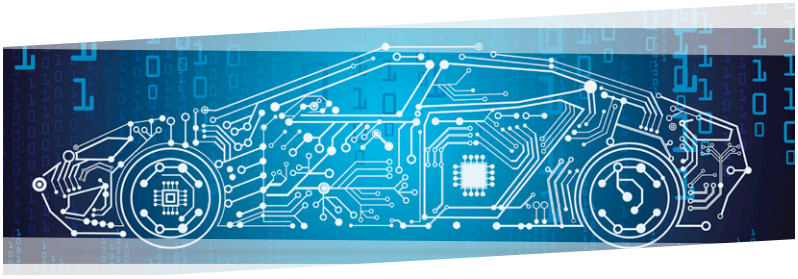
Geopolitical Impact on Cyber Threats from Nation-State Actors

This team explored the drivers, consequences, and scenarios associated with the emergence of marketplaces for sophisticated cyber tools and expertise. As part of the research process, the team interviewed over 50 stakeholders in the public and private sectors, including several noted experts, intelligence community analysts, and former US government officials.

The team's deliverable aims to influence how leaders and executives posture their organizations and support their security team's need to minimize surprise around the emergence of new cyber actors and effects. This research proposes a framework, a "grand arms cyber bazaar," to help distinguish among a growing range of actors, all having access to advanced capabilities, based on their organizational maturity (advanced, emerging, or opportunistic) and operational intent (collection, profit, or disruption). The deliverable also briefly touches on the privatization of digital surveillance, the vulnerabilities equities process, tiers of actors' capabilities, the balance of cyber power, and extant geopolitical tensions.

The knowledge and expertise shared during the team's research suggests several alternatives for how the global landscape may evolve in the next three years and identifies the factors that might shape each outcome. These insights into alternative futures can help executives and principals make efficacious investments in cyber security, in a challenging environment where many demands are being made for security resources.

Identifying Cyber Risks to Vehicle Technology Advancements



This team addressed the potential for cyber actors to exploit current and emerging technology in vehicles. Vehicle technology has come a long way since cars were first made affordable to the masses. Over a century since their introduction, vehicles that were previously closed systems comprised of analog components have been enhanced by the addition of complex interconnected systems. Vehicles are now dependent on systems of integrated circuits controlled by software to monitor and control vehicle functions, enabling greater safety, convenience, and efficiencies. As vehicles and supporting infrastructure become smarter, we must be aware of the risks associated with these advancements to ensure operational resilience.

Through their joint efforts, the team seeks to leverage the knowledge and skills of the private sector and the federal government to break down this complex landscape in an effort to establish a baseline understanding of the risks associated with the advancement of technologies, both obvious and subtle, in vehicles.

Industrial Internet of Things Interconnections

This team conducted research on the current Industrial Internet of Things (IIoT) landscape and its nexus to national security. In the late 1960's, the internet's predecessor—the Advanced Research Projects Agency Network (ARPANET)—was developed and successfully interconnected four university computers. ARPANET had been developed primarily to facilitate communications between people. By the end of 2019, over twenty-seven billion devices are expected to be connected as part of the vast confluence of technologies, platforms, protocols, standards, and devices known as the Internet of Things (IoT).

Among the multiplicity of sub-categories that now exists within this confluence is the IIoT. The IIoT is a group of interconnected devices that collect and transmit data within traditionally isolated industrial systems found in Supervisory Control and Data Acquisition systems and other Industrial Control Systems that monitor and control critical industrial infrastructure including factories, power plants, water systems, ports, and other industrial facilities, as well as certain U.S. and allied military systems. Critical infrastructure asset owners and operators are increasingly embracing the IIoT to enhance efficiency and optimize productivity, but the technology also brings cyber risks.

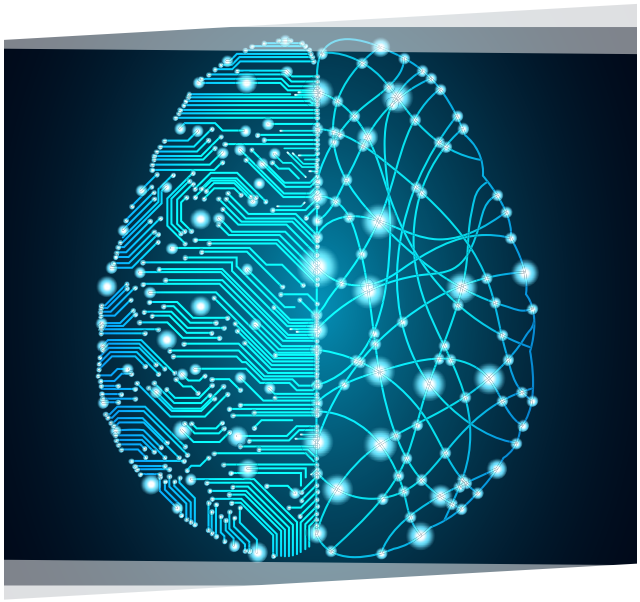
The team's deliverable aims to improve understanding of IIoT by providing an overview of the current IIoT landscape, the types of vulnerabilities and attacks that affect it, and public and private sector efforts to collaborate to implement and secure the IIoT, with special reference to the emergence of smart cities. The IoT and IIoT encompass broad technologies with exponentially expanding attack surfaces. While a complete cybersecurity solution exceeds the scope of this effort, the deliverable recommends areas for deeper future analysis.

Strategies to Address Physical Supply Chain Risks

This team focused on identifying best practices in maintaining integrity of the physical supply chain. Supply chain integrity pertains to the traceability of products within the supply chain, and their protection from modification or destruction. The team engaged with supply chain stakeholders from the pharmaceutical, food, and technology industries. The goal was to identify those parties in the public and private sectors that are exemplary in their success at maintaining integrity within the supply chain, and to generalize best practices based on these successes that can be broadly implemented to reduce supply chain risk and strengthen resilience.

The United States Government and large, multinational corporations utilize table top exercises to address existing and emerging security concerns within the extensive web of global supply chains, ensuring the integrity of products being delivered to wholesalers, retailers and consumers in the U.S. and abroad. The team extracted five key areas of best practice to consider while building a supply chain risk mitigation program and created exercise planning templates to share them: 1.) use a risk based approach aligned with the company's core values, 2.) build a network of internal and external subject matter experts, 3.) utilize modern monitoring technologies, 4.) collect data to analyze and map supply chain threats and disruption risks, 5.) enable a robust insider threat mitigation program in tandem with third party vetting procedures. These best practices, pulled from larger organizations with dedicated supply chain risk management programs, can guide smaller organizations which may not have the same level of resources available to assess and improve the integrity of their supply chains.

Artificial Intelligence (Phase II)



Recent advances in artificial intelligence (AI) have led to an explosion of multimedia applications for different domains such as commercial, industrial, and intelligence. Use of AI applications in national security, however, is often problematic because the opaque nature of the systems leads to an inability for a human to understand how the results came about. Reliance on "black boxes" to generate predictions and inform decisions is potentially disastrous. The AI team's research explores how the analytic tradecraft standards outlined in Intelligence Community Directive (ICD) 203 can provide a framework for assessing how well an AI system can explain the basis for its decisions (i.e. "analysis"). Providing the developer and user of an AI system with standards focused on the principles of good analysis adopted by the intelligence community can help promote the development of more understandable systems and engender greater trust in AI outputs.

Vulnerabilities of Healthcare Information Technology Systems (Phase II)

Building upon research and deliverables from the 2018 AEP, the Vulnerabilities of Healthcare Information Technology Systems team examined the nexus between patient safety and cybersecurity. A compromise of patient information, whether confidentiality, integrity, or availability may result in patient harm—physical, mental, financial, and otherwise. To this end, "patient safety" needs to be expanded to include cybersecurity and, specifically, confidentiality, integrity, and availability of patient information. Healthcare organizations need to be good stewards of patient information in light of these considerations.

Through a series of in-person and virtual meetings, private and public-sector healthcare cybersecurity subject matter experts provided valuable information on the current state of patient safety within the context of cybersecurity. The team's deliverable discusses the varying degrees of awareness of patient safety as it relates to cybersecurity and the state of progress regarding promoting patient safety through the lens of cybersecurity at healthcare provider organizations.

PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

Want to know more?

Please contact us with questions or concerns by email at AEP@hq.dhs.gov, or by phone at (202) 447-3673.

For more information, please contact us at:
AEP@hq.dhs.gov

This document is provided for educational and informational purposes only. The views and opinions expressed in this document do not necessarily state or reflect those of the U.S. Government or the Exchange Program Partners, and they may not be used for advertising or product endorsement purposes. All judgments and assessments are solely based on unclassified sources and are the product of joint public and USG efforts.

19-319-IA