2021 Public-Private Analytic Exchange Program Synopsis

PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

Contents

Background 1

Outcomes 1

2021 AEP Topic Team Abstracts 2

- Emerging Threats to Cargo and Port Security 2
- The Evolving Cyber Legal Landscape 2
- Importance of Private Sector Intelligence Programs 3
- Improving U.S. Competitiveness in the Global Market 3
- Increasing Threats of Deepfake Identities 4
- Privacy and Security Implications of 5G Technology 4
- Protecting Sensitive Data and Intellectual Property 5
- Threats to U.S. Food and Agriculture Sources 6

2021 AEP Phase II and III Topic Team Abstracts 7

- Best Practices in Vetting Prospective and Current Employees (Phase II) 7
- Combatting Disinformation Campaigns (Phase II) 7
- Vulnerabilities of Healthcare Information Technology Systems (Phase III) 8

Participants 9

- Private Sector 9
- Public Sector 9

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 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.

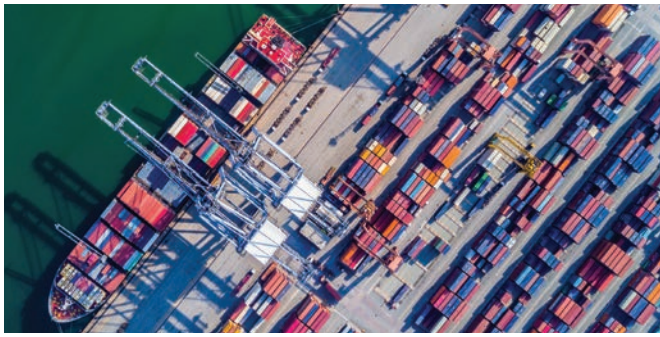
Outcomes

Past outcomes beyond the AEP include:

- All deliverables are disseminated to over 24,000 recipients via the Homeland Security Information Network and are posted on the DHS public website.
- In 2020, "Vulnerabilities of Healthcare Information Technology Security Systems" Phase II, 2019 Topic Team's analytic deliverables, "Phishing Don't Be Phool" and "A Lifeline Patient Safety and Cybersecurity" were sited during an industry panel inclusive of experts from Amazon Web Services, CrowdStrike, and, an AEP participant, (from the Healthcare Information and Management Systems Society) came together to analyze the attacks that occurred in 2020, discuss lessons learned, and what healthcare systems can do to prevent attacks in the future.
- In 2020, the DHS Transportation Security Administration opted to disseminate the "Strategies to Address Physical Supply Chain Risks" 2019 Topic Team's analytic deliverable to over 10,000 individuals in the public and private sector.
- In 2020, the DHS Information Security Training Working Group, chaired by the U.S. Immigration and Customs Enforcement, hosted a webinar featuring the 2018 AEP Topic Team "Vulnerabilities of Healthcare Information Security." The team presented its analytic deliverable findings, which provided a holistic perspective on phishing: what it is, the impact, and how to mitigate the phishing threat.
- Over the past few years, the Defense Intelligence Agency/Annual Defense Combating Terrorism Intelligence Conference has selected AEP Topic Teams participants as speakers or panelists to share in discussions with a variety of Department of Defense, U.S. Government, and international partner organizations on violent extremist organizations (VEOs) and key functions VEOs rely on.
- In late 2019, an Artificial Intelligence–Using Standards to Mitigate Risks Phase II Topic Team member was the keynote speaker on "AI in Public Health" at a Joint United Nations Program on HIV and AIDS.

2021 AEP Topic Team Abstracts

Emerging Threats to Cargo and Port Security



This team conducted research and analysis to identify critical risk areas within the cargo and port security sector. The team incorporated both government and private industry perspectives in developing and refining its assessment. Given the widely dispersed geographic nature of the cargo and port security realm, and the broad regional diversity of cargo and port security needs, the team chose to focus its efforts on a single, nationally significant subcomponent of the cargo and port security topic: drug trafficking.

During the team's exploratory research, drug trafficking organization (DTO) activities and maritime port security continually emerged as key areas of concern for most community stakeholders. Consequently, the following study is focused on threats posed by DTOs and their use of maritime ports to facilitate trafficking activities. Additionally, rather than focus on individual DTOs or specific drugs, the team chose to pursue a holistic approach aimed at analyzing DTO trafficking activities as a national-level threat vector in order to provide a practical risk assessment to identify those U.S. ports at greater risk of criminal exploitation. The team's risk assessment tool yielded a mix of both expected and unexpected results regarding the port facilities identified as most at risk for DTO exploitation.

In an effort to address the lack of an extensive, national-level assessment regarding DTO activities at maritime ports, the team formulated a comprehensive, purpose-built, risk-based prioritization tool, which can be used to inform the allocation of critical security resources to U.S. maritime port facilities across the country. Additionally, the team developed an informational slick sheet product to complement its risk assessment and serve as a resource for port security personnel and managers. In combination, this practical approach provided maritime port security stakeholders with a data-driven and actionable methodology for identifying risk and prioritizing resources to detect, deter, and mitigate DTO threats to their specific facilities.

The Evolving Cyber Legal Landscape

This team analyzed the facts, legal ramifications, and national security implications surrounding the practice of sharing deoxyribonucleic acid (DNA) through genetic testing. Team members accomplished this project by conducting analysis of current literature, participating in webinars, and interviewing experts in academia and the U.S. Government. The importance of this issue to U.S. national security has been underscored by the recent Biden Administration's Executive Order to protect Americans' privacy data from adversary threats.

This team's deliverable is a three-prong focus to educate, mitigate, and legislate. The intent of the first prong is to outreach to generations of Americans to "Educate Yourself" before considering genetic testing that does not protect DNA information. If, however, individuals have already shared their DNA information, deliberately or inadvertently, the second prong encourages readers to "Mitigate the Risk." Finally, the third prong urges lawmakers to "Legislate Safeguards" to protect Americans and U.S. national security from criminals and adversaries acquiring DNA databases for nefarious purposes.

Importance of Private Sector Intelligence Programs

This team assessed both public and private sector intelligence programs and conducted research to determine how private sector intelligence programs can provide critical capabilities within their parent organization's overall security apparatus. In recent years, the intelligence profession has expanded beyond the government sphere, and corporations worldwide have established their own internal intelligence programs.

The team's research included a review of existing literature on the nature and value of intelligence. The team gleaned further insights by surveying hundreds of individuals from the public and private sector who were involved in intelligence sharing, determining how intelligence programs are commonly structured and operated, perceived benefits and challenges of using an intelligence program, and recommendations for improving information sharing efforts.

Additionally, this team's deliverable includes appendices that highlight best practices from established corporate and government intelligence programs, such as how to use geospatial data, where to find credible info-sharing networks, and ways of setting realistic expectations with decision makers.

Improving U.S. Competitiveness in the Global Market

This team examined the current state of U.S. competitiveness in the global economy and provided recommendations on how the United States can improve and sustain its economic competitiveness, especially relative to other nations such as the People's Republic of China. It also explored how U.S. government agencies and U.S. private sector companies could work more closely to improve American competitiveness in the global market. To manage the complexity of multifaceted challenges to the U.S. economy and various industry sectors from competitors and foreign adversaries, it is essential for the government and its private sector partners to engage in true collaboration.

Increasing Threats of Deepfake Identities

This team conducted research on an emergent type of threat falling under the greater and more pervasive umbrella of synthetic media, which utilizes a form of AI to create believable, realistic videos, pictures, audio, and text of events that never happened.

Many applications of synthetic media represent innocent forms of entertainment, but others carry risk. The threat of deepfakes and synthetic media comes not from the technology used to create it, but from people's natural inclination to believe what they see; as a result, deepfakes and synthetic media do not need to be particularly advanced or believable in order to be effective in spreading mis/disinformation.

Based on numerous interviews conducted with experts in the field, it is apparent that the severity and urgency of the current threat from synthetic media depends on the exposure, perspective, and position of who you ask. The spectrum of concerns ranged from "an urgent threat" to "don't panic, just be prepared." To help customers understand how a potential threat might arise, and what that threat might look like, we considered several scenarios specific to the commerce, national security, and society arenas. The likelihood of any one of these scenarios occurring and succeeding will undoubtedly increase as the cost and resources needed to produce usable deepfakes simultaneously decreases—just as synthetic media became easier to create as non-AI techniques were made more available. In line with the multifaceted nature of the problem, there is no one or universal solution, though elements of technological innovation, education, and regulation must comprise part of any detection and mitigation measures.

In order to have success, there will have to be significant cooperation among stakeholders in the private and public sectors to overcome current obstacles, such as "stovepiping," and to ultimately protect ourselves from these emerging threats while protecting civil liberties.

Privacy and Security Implications of 5G Technology

This team examined new privacy and security implications associated with increasingly available fifth-generation (5G) wireless technology, which will radically improve the bandwidth, capacity, and reliability of mobile broadband. To identify areas of overlap and gaps in research, study, and action regarding 5G technology, the team developed a catalog of current and planned 5G security and privacy efforts of the U.S. government and private sector to determine what aspects of 5G security and privacy are being addressed and in what venues.

These findings were categorized into the following four major focus areas:

- 5G Standards;
- Cybersecurity and Supply Chain Security;
- Vendor Diversity and Economic Competition; and
- International Cooperation That Implicates 5G Security and Privacy.

Within each of these focus areas, the team documented existing key areas of work, including initiatives and resources developed by various federal departments and agencies, and analyzed them to identify recommendations for future public-private collaboration. Through these recommendations, the final deliverable harmonizes and de-conflicts overlapping 5G workstreams, addresses gaps in current efforts, and suggests public-private collaboration opportunities on vital 5G efforts to more efficiently deploy government and private sector resources.

Protecting Sensitive Data and Intellectual Property

This team assessed a range of topics along the lines of risks to sensitive data and intellectual property, including basic fundamentals, advanced techniques, and know-how. Virtually all organizations have sensitive data and intellectual property of some kind. Both are intangible assets that enhance the bottom line of every organization. Indeed, certain organizations depend upon the safeguarding of sensitive data and intellectual property in order to function. Sensitive data can be any kind of information that may require some sort of enhanced protection (e.g., classified information, confidential business information, privileged information, etc.). Intellectual property is defined by law and deals with information that essentially is a creation of the mind. Intellectual property includes, but is not limited to, copyrights, patents, trademarks, and trade secrets.

Thus, sensitive data and intellectual property must be protected using appropriate administrative, technical, and physical safeguards. Knowing what to do is only half the battle. Implementing best practices and mitigating risk are also necessary to adequately protect the information. Risks to sensitive data and intellectual property include the following: (1) dangers of foreign travel, (2) insider threat, (3) attack from external threat actors, and (4) supply chain integrity and security. While this list is non-exhaustive, these represent common scenarios in many organizations.

Threats to U.S. Food and Agriculture Sources

This team focused on a myriad of threats to the U.S. Food and Agriculture (FA) sector, which not only pose a persistent and imminent threat to plant, animal, and human health, but also have the potential to cause cascading impacts to the socio-political, economic, and health security of the United States. Gaps and vulnerabilities persist due to a lack of alignment and/or accountability to a variety of U.S. government research & development-oriented policy recommendations and a nonunified approach to sector-focused research requirements that aim to mitigate the threats and risks that directly impact food and agricultural systems and the interdependent critical infrastructure sectors that support the activities of the FA sector.

Technological convergence, including exponential experimental biology, could threaten agricultural production systems, the economy, and public health of the United States. Therefore, it is essential to understand critical gaps and vulnerabilities as we aim to bolster the awareness of, and the need for, risk-based, resilience-focused, research pursuits. The resulting recommendations require a concerted level of collaboration and coordination amongst the multitude of private industry, academic, non-governmental organization, and governmental agencies/departments that encompass the spectrum of normal operations, safeguarding activities, resilience initiatives, and regulatory oversight in the FA sector and are intended to:

- Inform how to allocate future public/private funding to academic, private, and national research facilities that perform activities to mitigate threats and reduce risk within the FA sector;
- Educate and encourage the involvement of private sector stakeholders in order to leverage and foster a holistic pursuit of prioritized areas of interest and ensure research will support enterprise-wide, risk-reducing resources, tools, or programs;
- Develop a sustainable model for securing and ensuring funding of targeted research to mutually benefit all stakeholders in the FA sector, while protecting the nation's food supply and associated supply chains; and
- Provide forward-looking solutions to imminent threats and hazards, such as those posed by the accelerated natural evolution of pathogens that pass between humans, domestic animal/plant populations, and wildlife or the accidental or intentional release of laboratory-manipulated pathogens that are becoming more prevalent due to minimal safeguards and unregulated technological advancements.

2021 AEP Phase II and III Topic Team Abstracts

Originating prior to AEP 2020, these Topic Teams identified areas to further explore and requested to continue their research efforts.

Best Practices in Vetting Prospective and Current Employees (Phase II)

This team proposed five recommendations based on its 2019 research and analysis organized in the following themes: organizational culture, recurrent and continuous vetting, standardized processes, collaboration across industries, and criticality of speed. In 2021, the team's research focused on developing a greater understanding of one of these themes. Specifically, the research focused on understanding how organizational culture and values impact hiring and retaining employees while reducing enterprise risk.

The team developed standardized questionnaires for small to medium sized businesses and conducted a series of interviews with company executives, security professionals, hiring professionals and managers, and companies that specialize in recruiting. While culture and values play a central role during employee interviews, the team discovered additional tools and best practices that would enhance the hiring and retention process. Key among them was embracing culture and values throughout all phases of an employee's lifecycle, the use of social media in vetting candidates, and the use of personality assessment instruments prior to hiring. When these best practices were identified, the team sought out and interviewed government and private sector experts to gain a better understanding of how these tools are utilized currently and where they could augment the employee lifecycle and minimize enterprise risk. The results of this research are a series of job aides that small- to medium-sized organizations can use to ensure culture and values are incorporated into all aspects of the employee lifecycle.

Combatting Disinformation Campaigns (Phase II)

This team examined methods of reducing the supply of, and demand for, disinformation. In recent years, disinformation has impacted national security, undermined the foundations of civil society, and made it more difficult to find common solutions to a wide variety of issues facing contemporary society, from climate change to pandemic response. Attempts to counter disinformation frequently run into technological, legal, ethical, and political obstacles. Governmental entities are constrained in their ability to curb disinformation from domestic

threat actors and private sector entities can benefit from allowing disinformation to flourish on the platforms that they own. The polarization of U.S. society provides fertile ground for the spread of disinformation. If an audience for disinformation exists, threat actors will provide a steady supply. Eliminating disinformation completely is an unattainable goal. However, the team's research indicates that there are measures that can slow down the proliferation of disinformation and help to reduce the impact of targeted disinformation campaigns. In this deliverable, the team will evaluate the feasibility of measures that have been proposed for future implementation, or have been implemented in the past, and will then make recommendations regarding courses of action that are most likely to bear fruit.

Vulnerabilities of Healthcare Information Technology Systems (Phase III)

This team continued examining threats and vulnerabilities in the healthcare landscape with a direct focus on consumer health technology and its associated risks. Consumer healthcare technology offers several benefits for consumers and patients. Opportunities exist where consumers may capture their biometric data with consumer healthcare equipment and share that data to have meaningful conversations with their care providers.

While benefits abound, and technology offers society many potential benefits, risks exist as well. Consumer healthcare devices may integrate with home Internet of Things (IoT) devices, capture geolocation data, or include consumer information that extends beyond what the consumer may be aware of. Consumer healthcare devices are not medical devices in terms of regulatory definitions. As such, device manufacturers may assemble devices and develop functionality that may not employ the same rigors as when developing medical devices. Further complications arise post purchase for the ongoing cyber hygiene of such devices (i.e., patching of software, operating systems, or component firmware). Yet, these devices may offer mobile interoperability and interconnect with various systems.

This project researched the threat and risk scope for consumer healthcare technology and potential mitigation concepts. Healthcare technology evolves at a rapid pace; consumer healthcare technology is one aspect of that evolution. As society embraces technology to better our lives, we need to consider external implications. This research effort explores issues that may arise from potential, unintended consequences and offers thoughts to build a safer consumer experience by ensuring the security of digital platforms.

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

DECEMBER 2021 21-287-IA