ASPEN TECH POLICY HUB

PROJECT

Photo by Bernard Hermant via Unsplash

STEVE WEIS

AMINA ASMIN

ALONI COHEN

Classified Threat Sensors for National Security

How the intelligence community can help American industry defend itself from foreign adversaries

EXECUTIVE SUMMARY

Foreign nation-state cyberattacks against US-based companies create a national security risk and the potential loss of intellectual property. Yet industry and government struggle to engage in data-sharing that could mitigate these risks due to the sensitive nature of classified data. Recent developments in secure enclave technology could help companies and government act on classified intelligence without requiring declassification. This project recommends using secure enclaves to operate classified threat sensors on the servers of private companies. These threat sensors would be able to scan a company's local security data for signs of cyberattack without revealing the company's proprietary data, or the information that the sensors were searching for. The project recommends a measured rollout to pilot this new technology.

To learn more about this project, please visit aspentechpolicyhub.org.

THE ASPEN INSTITUTE

THE PROBLEM

Foreign nation-state cyberattacks against US-based companies create a national security risk and result in the loss of competitive intellectual property. The US intelligence community holds classified information that could help detect nation state attacks. However, that intelligence cannot be shared without risking sources and methods. Private security data held by industry, which might not be accessible due to regulatory or public perception issues about sharing data with governments, could in turn aid intelligence agencies in identifying broader attack campaigns.

> *Classified threat sensors built with off-the-shelf technology solve the information sharing challenge without declassifying intelligence or exposing private data to governments.*

THE SOLUTION

Classified threat sensors solve the information sharing challenge without declassifying intelligence or exposing private data to governments. They may be built from off-the-shelf technology using existing open source tools. These sensors could speed detection and attribution of cyberattacks by foreign powers. They can also act as an early-warning system to discover broader campaigns, without exposing private company data to the government. To implement this solution, this project recommends a phased trial between the NSA, DHS, and private industry partners—running parallel trial deployments for both industry-to-industry and government-to-government sharing. After proven in trials, a government-to-industry sharing program could be deployed between DHS and industry partners.

ASPEN TECH POLICY HUB

PROJECT

ABOUT THE HUB

The Aspen Tech Policy Hub is a Bay Area policy incubator, training a new generation of tech policy entrepreneurs. We take tech experts, teach them the policy process, and support them in creating outside-the-box solutions to society's problems.

The Aspen Institute
2300 N St. NW, Suite 700
Washington, DC 20037
202 736 5800

THE ASPEN INSTITUTE