



DoD CYBER CRIME CENTER (DC3)

Operations Enablement Directorate

OED FACT SHEET



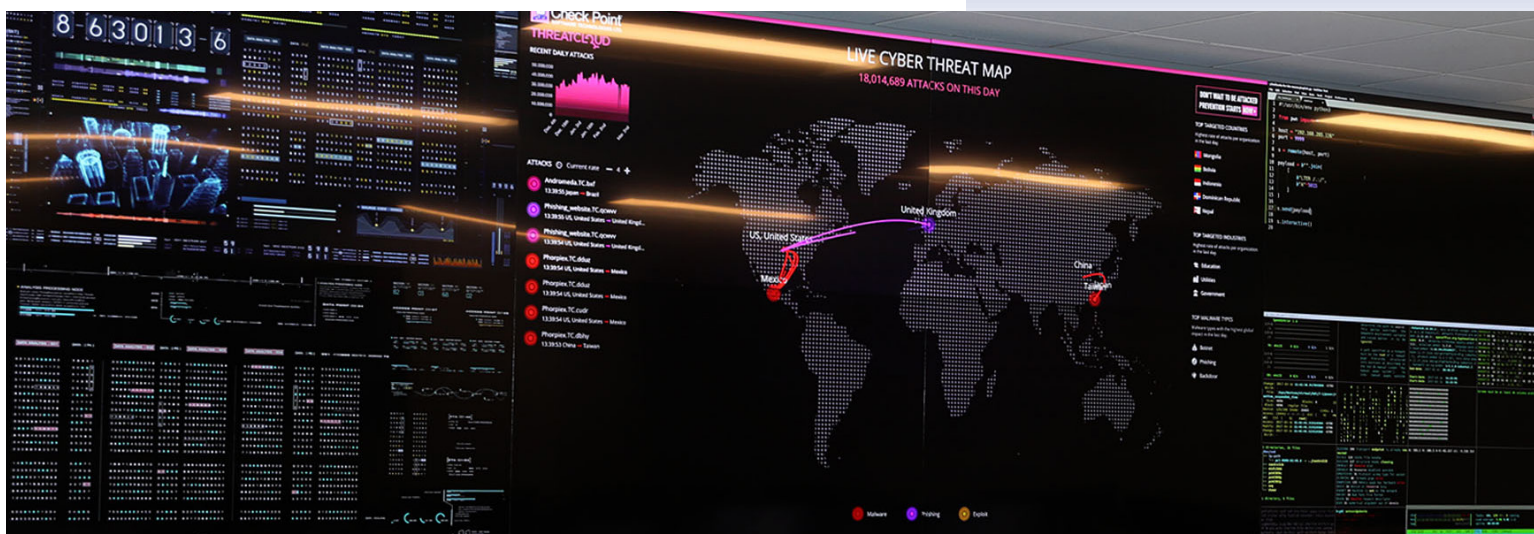
Operations Enablement Directorate (OED)

The mission and principal focus of the OED is to amplify the effects of DoD-wide law enforcement and counterintelligence (LE/CI) investigations and operations, and by extension, the effects of the U.S. Intelligence Community at large. That charge encompasses:

1. Conducting expert technical and all-source analysis (resulting in more than 493 products released in FY21) focused on countering foreign intelligence threats to DoD and the U.S. government as a whole
2. Integrating disparate and emerging technologies to enhance collaboration, interoperability, and the collective capabilities of DoD and Federal LE/CI, cybersecurity, and acquisition communities
3. Providing focused oversight and integration with the LE/CI and intelligence communities through liaison officers and embeds with:
 - Air Force Life Cycle Management Center (AFLCMC)
 - Army Military Intelligence
 - U.S. Cyber Command
 - Defense Counterintelligence and Security Agency (DCSA)
 - FBI
 - National Cyber Investigative Task Force (NCIJTF)

2020–2022 National Counterintelligence Strategy Objectives:

- Protect the nation’s critical infrastructure
- Reduce threats to key U.S. supply chains
- Counter the exploitation of the U.S. economy
- Defend American democracy against foreign influence threats
- Counter foreign intelligence cyber and technical operations



OED CAPABILITIES

Analytical Group (AG)

The mission of the AG is to conduct sharply focused technical and cyber intelligence analysis, leveraging multiple sources of data, unique analytic tools, applications, and capabilities to directly support stakeholder requirements and priorities.

Production – The AG publishes reports that result in numerous investigational and operational leads and technical findings, and highlight trends that enable predictive analysis, including:

- Cyber Intelligence Reports (highlights of activities/trends to enable predictive analysis)
- Cyber Profiles (summaries of entity findings with attribution supporting LE/CI cyber investigations and operations)
- Intelligence Information Reports
- Operational Lead Reports (summaries of technical findings, including identification of new operational leads)
- Cyber Intelligence products issued jointly with multiple Government Agencies and Partners.

Collaboration – The AG partners with the DC3 Defense Industrial Base (DIB) Collaborative Information Sharing Environment and the DC3 Cyber Forensics Lab to protect critical technologies and information, and is central to the release of malware signatures and decoders which allow DIB partners to defend their networks from malicious actors.

AG Quarterly Meeting – The AG hosts attendees from DoD and federal-level law enforcement and cyber agencies to discuss relevant and emerging cyber threat items of interest.

Capability Integration Group (CIG)

The CIG identifies opportunities to leverage existing DOD resources across multiple mission spaces to create unique vantage points to counter adversary intent. The CIG mission supports DoD operations and requirements through development and management of the Collect, Analyze, Disseminate and Operationalize - Integrated Solution (CADO-IS) and Automated Data Obfuscation (ADO) system.

- **CADO-IS** - CIG leads the integration of multiple fused data sources and analysis across Military Department CI Organizations, DoD Components, and other key partners through the development and stand-up of CADO-IS.
- **ADO System** – CIG manages the development, sustainment and enhancement of automated data obfuscation to defend DoD and the Defense Industrial Base from criminal and nation state threat actors.