A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER

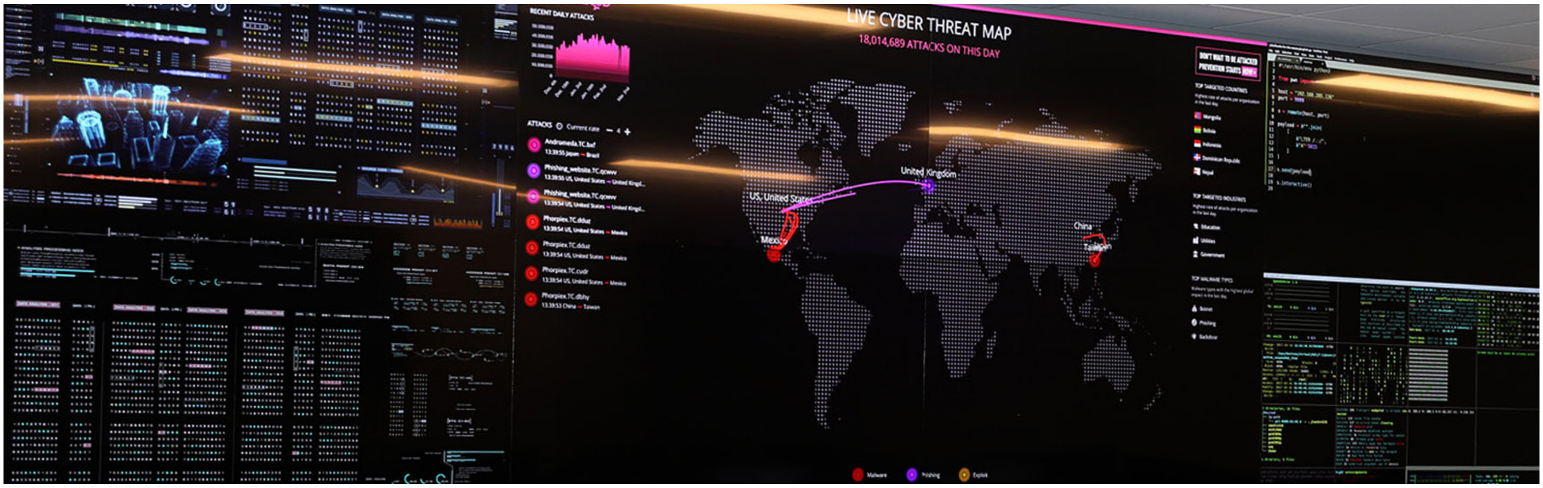
Operations Enablement Directorate (OED)

The principal focus of the **Operations Enablement Directorate (OED)** is to amplify the effects of DC3 capabilities and data sources to illuminate unique cyber risks and opportunities in support of U.S. government partners, DoD-wide law enforcement and counterintelligence (LE/CI) investigations and operations, and the U.S. Intelligence Community at large. This charge includes:

1. Conducting expert technical and all-source analysis focused on countering foreign intelligence threats to DoD and the U.S. government as a whole
2. Development of serialized intelligence products derived from analytical research of numerous data sources to enhance U.S. government cyber threat landscape
3. Integrating disparate and emerging technologies to enhance collaboration, interoperability, and the collective capabilities of DoD and Federal LE/CI, cybersecurity, and acquisition communities
4. 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)

2023 National Intelligence Strategy Vision:

An Intelligence Community that embodies America's values and is sufficiently agile, integrated, innovative, and resilient to inform national security and foreign policy decisions, resulting in a Nation that is secure and prosperous.



OED CAPABILITIES

OED consists of two teams: the **Analytical Group (AG)** and the **Special Capabilities Group (SCG)**.

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, language-enabled analysts, applications, and capabilities to directly support stakeholder requirements and priorities.

Collaboration

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.

Production

The AG publishes reports that result in numerous investigation 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.

Special Capabilities Group (SCG)

SCG identifies opportunities to leverage existing DOD resources across multiple mission spaces to create unique vantage points to counter adversary intent. The SCG focus is to develop and field innovative, cross-cutting capabilities to support DC3's mission partners and support DoD operations and requirements.

over **400**

analytic engagements with U.S. Government Partners

over **200**

Finished Intelligence citations across the interagency

Pub. Date 10 MARCH 2025