A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER (DC3)

Operations Enablement Directorate

OED FACT SHEET

Operations Enablement Directorate (OED)

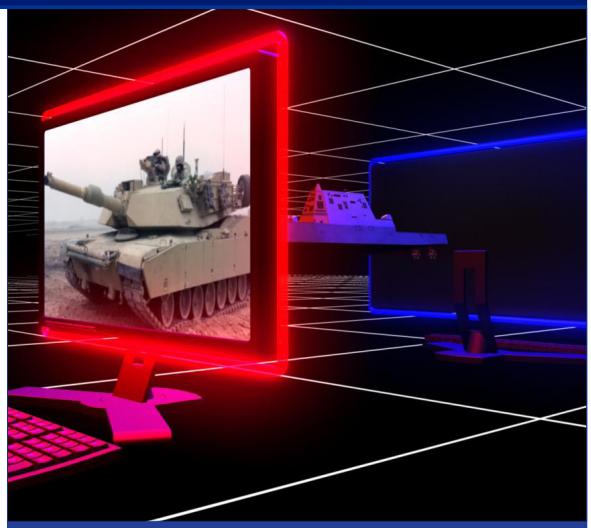
OED's mission and principal focus is to amplify the effects of DoD-wide Law Enforcement and Counterintelligence (LE/CI) investigations and operations, and by extension, the effects of the U.S. Intelligence Community at large. That charge encompasses:

1) Conducting expert technical and all source analysis resulting in over 510 products focused on countering foreign intelligence threats to DoD and the U.S. government in FY20.

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) Focused oversight and integration with the LE/CI and intelligence communities through liaison officers and embeds with:

- Air Force Cyber Resiliency Office for Weapons Systems (CROWS)
- Army Military Intelligence
- U.S. Cyber Command
- Defense Counterintelligence and Security Agency (DCSA)
- FBI's Baltimore Field Office
- National Cyber Investigative Task Force (NCIJTF)



- ***Counter foreign intelligence cyber and technical operations***
- ***Reduce threats to key US Supply chains***
- ***Counter the exploitation of the U.S. economy***
- ***Defend American democracy against foreign influence***

***2020* National Counterintelligence Strategy Objectives**

DoD CYBER CRIME CENTER
410-981-6610 | www.dc3.mil | info@dc3.mil
@DC3Forensics
@DC3 Cyber Crime Center

OED CAPABILITIES

Analytical Group (AG)

The AG's mission 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.

AG publishes – reports that have resulted in numerous investigational and operational leads, technical findings and highlighted trends that enable predictive analysis, including:

- Cyber Intelligence Reports–highlighting activities/trends to enable predictive analysis
- Cyber Profiles–summary of entity findings with attribution supporting LE/CI cyber investigations and operations
- Intelligence Information Reports
- Operational Lead Reports–summary of technical findings; identification of new operational leads

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

AG's Quarterly Meeting – 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's mission is to support joint operations and DoD-wide capabilities cutting across services including StormSystem and Collect, Analyze, Disseminate and Operationalize-Integrated Solution (CADO-IS).

CIG Manages – the development, sustainment and enhancement of StormSystem to defend DoD and the Defense Industrial Base from criminal and nation state threat actors.

CIG Leads – the integration of critical threat data and analysis across Military Department CI Organizations, DoD Components, and other key partners through the development and stand-up of CADO-IS.

CIG Integrates – across the US government working closely with the Office of the Undersecretary of Defense for Intelligence and Security and the CI community to define and prioritize new technical capability development.