Deputy Under Secretary of the Navy (Intelligence & Security)

Security Education Bulletin - March 2024

"Know Thy Enemy" - *Sun Tzu*

The security environment is defined by diverse threats and challenges, which include nation-state militaries, foreign intelligence actors, terrorists, smugglers, proliferators, transnational criminals, insider threats and even pirates. In order to successfully counter adversaries and fight our enemies, we must first know who they are. This includes the identification of state-sponsored actors engaging in espionage at home and abroad, foreign military personnel and experts attempting to steal critical technology, proliferators of weapons via sea lanes, and stateless actors who threaten the freedom of the seas.

By establishing identity and attributing actions, we deny our adversaries anonymity and can better safeguard Department of the Navy assets and information, secure our installations, protect our warfighters and their families, and defend our Nation.

What are Identity Activities?

These capabilities identify and link individuals, networks and nations to actions, events, and locations. *Identity Activities* uncover threats and distinguish friend from foe. For example:

Biometrics including fingerprints, facial recognition or DNA, can contribute to the establishment of a trusted workforce or identify a foreign counterintelligence threat at the gate.

Forensics is the scientific analysis of physical items and places; it uses laboratories and other facilities, personnel, and technologies to support the recognition, collection, preservation, analysis, storage, and sharing of forensic materials and data. This includes latent fingerprints, DNA, chemical analysis and other disciplines that can irrefutably link responsible parties to events and places.

Document and media exploitation can give an operational commander insight into the thoughts and plans of an adversary through the extraction of information and intelligence from captured enemy documents and media.

Digital and multimedia forensics exploits digitized files and evidence related to computer intrusions, terrorist cell planning, unauthorized disclosure of classified information, or other events involving cellphones, hard drives and computers. Devices can be exploited for images, audio, and video to extract information.

Why does it matter to you?

Identity Activities enables security, law enforcement, force protection/anti-terrorism, intelligence and counterintelligence to prevent and deter malicious actors. They assist in ensuring we retain a competitive edge, the advantage at sea, and maintain the world's greatest naval force!

document & media exploitation

biometrics **IDENTITY FORENSICS**

digital & multimedia forensics

Check out these resources to learn more about Identity Activities

The Defense Forensics and Biometrics Agency (DFBA) was established as the Defense Executive Agent to ensure DoD keeps pace with rapidly evolving technologies:
https://www.dfba.mil/

NCIS Technical Service Field Office, Identity Activities (TSFO-IA) protects Department of the Navy assets, facilities, and warfighters through use of Identity Activities:
https://www.ncis.navy.mil/Mission/Mission-Support/Biometrics/

Marine Corps forensics is enhancing its capabilities to better gather vital data:
https://www.marines.mil/News/News-Display/Article/1789959/marine-corps-enhances-forensics-capability-to-make-gathering-data-simple/

This product was published by the Deputy Under Secretary of the Navy (Intelligence and Security), Security Directorate, to enhance a *Security Culture* through awareness and education.