Anti-Piracy

Proficiency Code: A

Cyber threats come in many forms. They range from hackers intent on the piracy and theft of intellectual property to well-organized campaigns by state and nonstate actors to exploit national secrets, deny service or bring down vital military networks.

Intellectual property theft involves robbing people or companies of their ideas, inventions, and creative expressions—known as "intellectual property"—which can include everything from trade secrets and proprietary products and parts to movies, music, and software.

It is a growing threat—especially with the rise of digital technologies and Internet file sharing networks. And much of the theft takes place overseas, where laws are often lax and enforcement is more difficult. All told, intellectual property theft costs U.S. businesses billions of dollars a year and robs the nation of jobs and tax revenues.

Preventing intellectual property theft is a priority of the Federal Bureau of Investigations (FBI) criminal investigative program. It specifically focuses on the theft of trade secrets and infringements on products that can impact consumers' health and safety, such as counterfeit aircraft, car, and electronic parts. Key to the program's success is linking the considerable resources and efforts of the private sector with law enforcement partners on local, state, federal, and international level.

Operation Chain Reaction, an initiative by the National Intellectual Property Rights Coordination Center (NIPRCC), is a comprehensive effort that targets counterfeit goods entering the supply chains of the Department of Defense (DoD) and other U.S. government agencies. Chain Reaction began in June 2011 to combat the proliferation of counterfeit goods into the DoD and federal government supply chains. While individual agencies have focused on counterfeit and misbranded items entering the federal supply chain, Chain Reaction is the first time that NIPRCC participants have collectively addressed this ongoing problem. As a task force, the NIPRCC uses the expertise of its member agencies to share information, coordinate enforcement actions, and conduct investigations to protect the public's health and safety, the U.S. economy, and the war fighters.

Some examples of recent investigations involving counterfeit products entering the federal supply chain include:

- An investigation uncovered the purchase of counterfeit Cisco converters by an individual, who intended to sell them to the DoD for use by the Marine Corps to transmit troop movements, rely intelligence and maintain security for a military base.
- An investigation uncovered a global procurement and distribution network based in California that provided counterfeit integrated circuits to various governmental agencies, including the military and prime DoD contractors. Agents conducted undercover purchases from individuals

within the company under official navy contracts and were provided counterfeits for various weapon platforms.

- An investigation identified a Florida-based electronics broker providing counterfeit integrated circuits to a prime DoD contractor fulfilling a Navy contract for components destined for implementation into ship and land based antennas.

Source material:

https://www.af.mil/News/Article-Display/Article/109583/pacom-promotes-regional-cyber-capabilities-defenses/

https://www.fbi.gov/investigate/white-collar-crime/piracy-ip-theft

Additional Information:

https://usaf.dps.mil/teams/10445/LPL/Documents/3DXXX%20-%20Cyberspace%20Support/Intellectual-Property-Protection-Brochure.pdf