Ethical Hacking and Countermeasures

Version 6

Module LXIV

Economic Espionage

Economic Espionage Suspect Sentenced in Plea Deal

By David Kravets ✉ June 18, 2008 | 3:13:01 PM Categories: Crime

A California man on Wednesday became the nation's first person sentenced under a rarely used economic espionage charge, a plea deal scuttling inferences the Chinese government may have engaged in economic espionage against the United States.

Xiadong Sheldon Meng, 44, pleaded guilty last year to two charges of attempting to sell fighter-pilot simulation software to the Chinese Navy. He is among five defendants nationwide charged under the Economic Espionage of 1996 for assisting foreign governments.

Meng's espionage included the misappropriation of a trade secret, known as "Mantis 1.5.5," from his former employer, Quantum3D of San Jose, with intentions of assisting a foreign government. The Quantum3D product simulates real-world motion for military training.

The government said Meng, who faced a life sentence without the plea deal, installed a "demonstration unit" of the software at China's Navy Research Center.

Under a carefully crafted plea deal, the government dropped all theft charges. The legal jockeying was a form of international relations of sorts. It eliminated the question of whether the Chinese military knew the software was stolen and was therefore engaged in economic espionage.

But instead of creating an international crisis, the government allowed the defendant to plead guilty to exporting a software program that might benefit a foreign government. He also pleaded guilty to exporting military source code without a license required under the Arms Export Control Act.

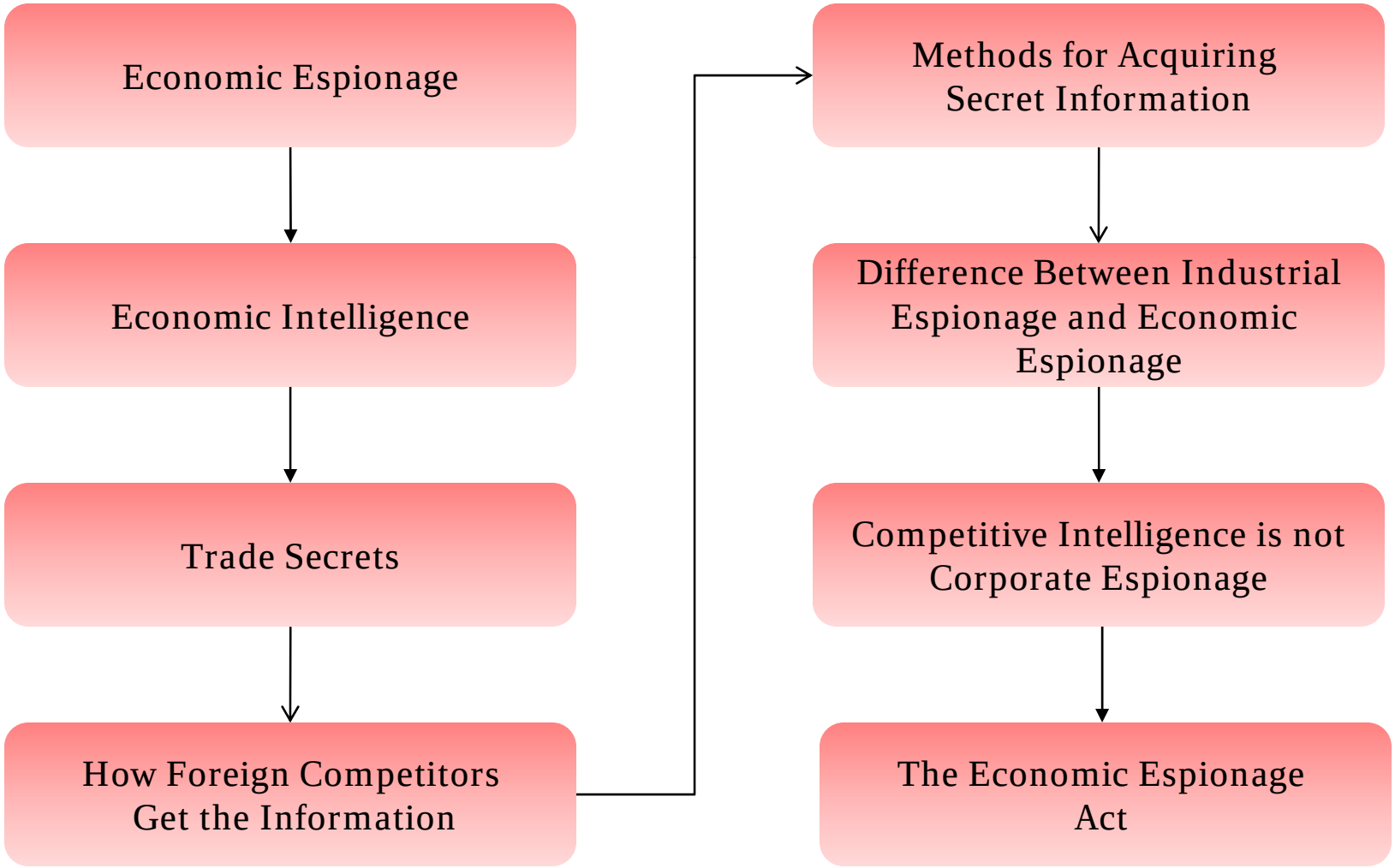
Source: *http://blog.wired.com*

Module Objective

This module will familiarize you with:

- Economic Espionage
- Economic Intelligence
- Trade Secrets
- How Foreign Competitors Get the Information
- Methods for Acquiring Secret Information
- Difference Between Industrial Espionage and Economic Espionage
- Competitive Intelligence is not Corporate Espionage
- The Economic Espionage Act

Module Flow



"Economic Espionage is the greatest threat to our national security since the Cold War"

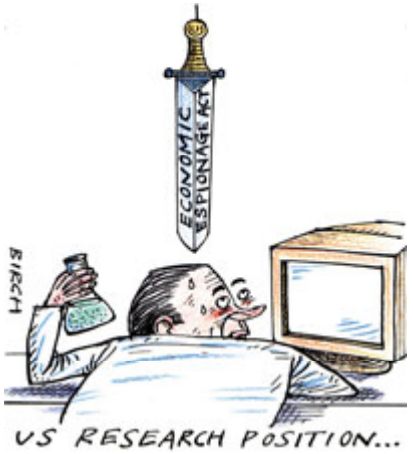
-- Louis Freeh, former FBI Director

Economic Espionage

According to FBI, "Whoever knowingly performs targeting or acquisition of trade secrets or knowingly benefits any foreign government, foreign instrumentality, or foreign agent is termed as Economic Espionage"

It may be considered as a new form of the white-collar crime that comprises cybercrimes and technology-related crimes

Foreign Agent may be anyone such as any officer, employee, proxy, servant, delegate, or representative of a foreign government



Who are Behind This?

- Competitors
- Vendors
- Investigators
- Business intelligence
- Consultants
- The press
- Labor negotiators
- Government agencies

Motives

To acquire new technologies

To advance a military program

To advance the economic competitiveness of the nation's industrial base

Economic Intelligence

According to CSIS, "Economic Intelligence is a policy or secret or commercial information, the acquisition of which by foreign interests either directly or indirectly can assist the relative productivity or competitive position of the economy of the collecting organization's country"

Economic intelligence may include technological data, financial, proprietary commercial, and government information

Trade Secrets

Trade secrets or information having threat from economic espionage are:

- Financial
- Business
- Scientific
- Technical
- Economic or engineering information
- Plans
- Program devices
- Formulas
- Designs
- Prototypes
- Codes whether tangible or intangible
- Proprietary technology or critical technology

How Foreign Competitors Get the Information

Foreign competitors aggressively target and recruit susceptible people (often from the same national background) working for domestic companies and research institutions

They recruit people to locate economic intelligence through operations like bribery, discreet theft, dumpster diving, and wiretapping

They establish seemingly innocent business relationships between foreign companies and domestic industries to gather economic intelligence including the classified information

Methods of Acquiring Trade Secrets

Steal, conceal, or carry away by fraud, artifice, or deception

Copy, duplicate, sketch, draw, photograph, download, upload, alter, destroy, photocopy, replicate, transmit, deliver, send, mail, communicate, or convey

Receive, buy, or possess a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization

How Economic Espionage Increases

- Transfer of information at high speed over the Internet
- Rapid development of computer and telecommunications technology
- Technological Challenges and New Vulnerabilities
- Security technology will always continue to be a step or two behind the attackers
- Lack of management support to provide better security as a higher priority
- Conflicting Laws and Investigatory Challenges

Difference Between Industrial Espionage and Economic Espionage

The major difference between economic espionage and industrial espionage is that the economic espionage may involve a government's effort to collect information

Economic Espionage occurs between nations

Competitive Intelligence

Competitive intelligence is the systematic and ethical process of gathering, analyzing and managing information about your competitors from different resources

It includes:

- Structural analysis of industries
- Investigation of industry competition through the study of rivalry among competitor firms
- Bargaining of relationships between buyers and suppliers
- Substitutability of products and services

Competitive Intelligence Is Not Corporate Espionage

Corporate espionage refers to the use of illegal means to gather information

It becomes illegal when it involves the theft of information or trade secrets

The Economic Espionage Act of 1996, 18 U.S.C. §§ 1831-1839

- The Economic Espionage Act of 1996 ("EEA") criminalizes two types of trade secret misappropriation in Title 18. Section 1831punishes the theft of a trade secret to benefit a foreign government, instrumentality, or agent:
  - (a) In general.—Whoever, *intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—*
    - (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;
    - (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;
    - (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
    - (4) attempts to commit any offense described in any of paragraphs (1) through (3); or
    - (5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

    shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both.

Source: *http://www.usdoj.gov/*

Methods for Economic Espionage Protection

- Recognize there is a real threat
- Identify and evaluate trade secrets
- Implement a definable plan for safeguarding trade secrets
- Secure physical trade secrets and limit access to the trade secrets
- Confine intellectual knowledge
- Provide ongoing security training to employees

Summary

- Whoever knowingly performs targeting or acquisition of trade secrets or knowingly benefits any foreign government, foreign instrumentality, or foreign agent is termed as Economic Espionage
- Economic intelligence may include technological data, financial, proprietary commercial, and government information
- Competitive intelligence is the systematic and ethical process of gathering, analyzing, and managing information about your competitors from different resources
- Corporate espionage refers to the use of illegal means to gather information