Economic Espionage

Marc Violante

Wisconsin Procurement Institute

April 29, 2020

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

Alternate title

They want, what you have!

Federal Government - programs

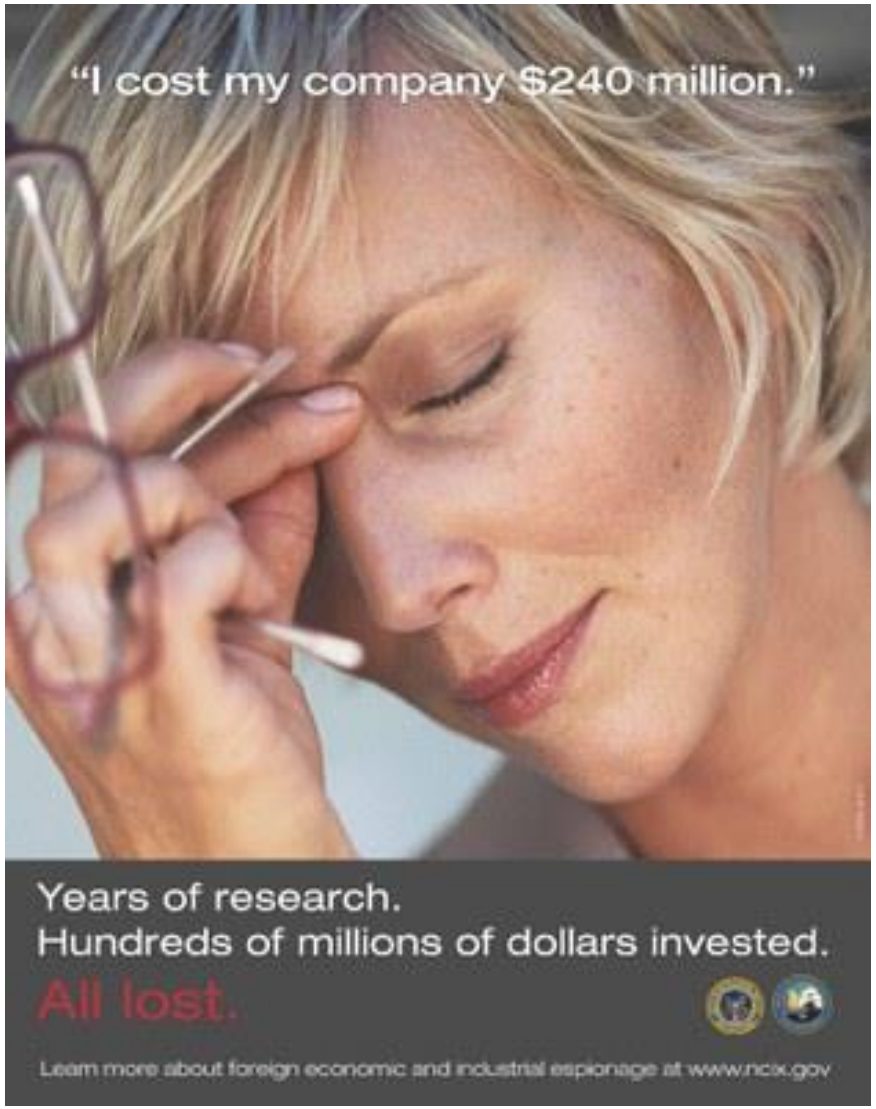
I have a secret – Of course, everyone wants to know it.

- FOUO
- Federal Contract Information (FCI)
- Controlled Unclassified Information (CUI – Basic/Specified)
- Joint Certification Program
- International Traffic in Arms (ITAR)
- Export Administration Regulations (EAR)
- Classified programs/information

Targeted Industries or Sectors

- Information and communication technology
- Business information that pertains to supplies of scarce natural resources or that provides global actors an edge in negotiations with U.S. businesses or the U.S. government
- Military technologies (marine systems, unmanned aerial vehicles, and aerospace/aeronautic technologies)
- Civilian and dual-use technologies in fast-growing sectors (clean energy, health care and pharmaceuticals, and agricultural technology)

https://www.fbi.gov/file-repository/economic-espionage-508.pdf/view



https://www.dsac.gov/topics/image-repository/economic-espionage.jpeg/

How might this happen?

Northern District of California

FOR IMMEDIATE RELEASE

Friday, September 7, 2018

Four Chinese State-Owned Industrial Companies Arraigned In Economic Espionage Conspiracy

The trade secrets relate to TiO2 technology from DuPont. DuPont had developed the technology and controlled a significant amount of the world's TiO2 sales. The defendants are alleged to have obtained confidential trade secret information including photographs related to TiO2 plant technologies and facilities. Further, the defendants are alleged to have paid an Oakland company at least $27,000,000 between 2006 and 2011 for assistance with TiO2 technology, including obtaining DuPont trade secrets. The defendants also allegedly attempted, between 2008 and 2011, to commit economic espionage related to DuPont's TiO2 processes.

https://www.justice.gov/usao-ndca/pr/four-chinese-state-owned-industrial-companies-arraigned-economic-espionage-conspiracy

Why?

Northern District of New York

FOR IMMEDIATE RELEASE

Tuesday, April 23, 2019

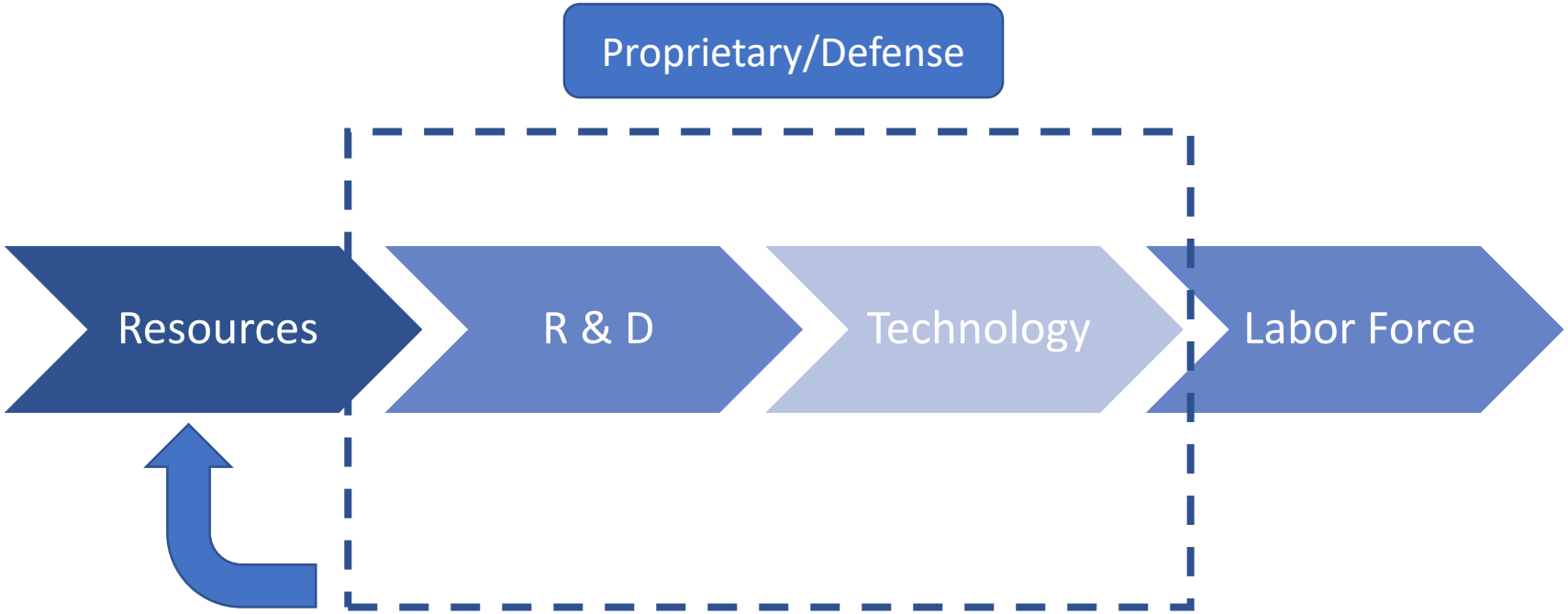
Former GE Engineer and Chinese Businessman Charged with Economic Espionage and Theft of GE's Trade Secrets

The Pair Allegedly Conspired to Steal GE's Trade Secrets for Use in Their China-Based Companies to Benefit the People's Republic of China

"The indictment alleges a textbook example of the Chinese government's strategy to rob American companies of their intellectual property and to replicate their products in Chinese factories, enabling Chinese companies to replace the American company first in the Chinese market and later worldwide," said Assistant Attorney General Demers. "We will not stand idly by while the world's second-largest economy engages in state-sponsored theft. As part of the Attorney General's China Initiative, we will partner with the private sector to hold responsible those who violate our laws, and we urge China's leaders to join responsible nations and to act with honesty and integrity when competing in the global marketplace."

https://www.justice.gov/usao-ndny/pr/former-ge-engineer-and-chinese-businessman-charged-economic-espionage-and-theft-ge-s

What drives economic success?

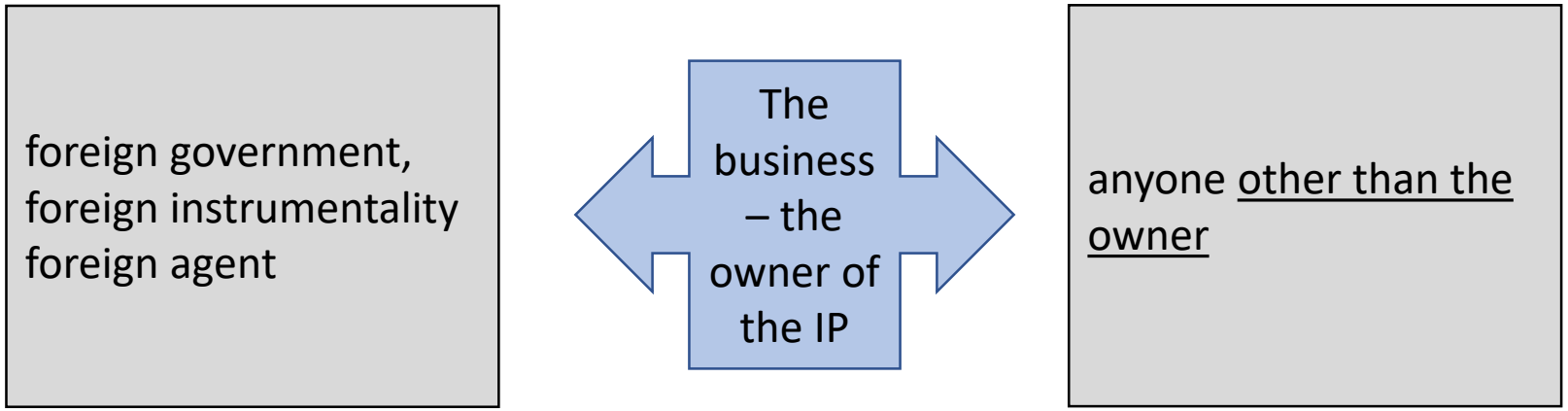


What is “economic espionage”?

- According to the Economic Espionage Act (Title 18 U.S.C. §1831), economic espionage is (1) whoever knowingly performs targeting or acquisition of trade secrets to (2) knowingly benefit any foreign government, foreign instrumentality, or foreign agent. In contrast, the theft of trade secrets (Title 18 U.S.C. Section 1832) is (1) whoever knowingly misappropriates trade secrets to (2) benefit anyone other than the owner.
- Historically, economic espionage has targeted defense-related and high-tech industries. But recent FBI cases have shown that no industry, large or small, is immune to the threat. Any company with a proprietary product, process, or idea can be a target; any unprotected trade secret is vulnerable to theft by those who wish to illegally obtain innovations to increase their market share at a victim company’s expense.

https://www.fbi.gov/investigate/counterintelligence

What is the common denominator?



Recent cases

FOR IMMEDIATE RELEASE Thursday, March 19, 2020

Former Uber Self-Driving Car Executive Signs Agreement To Plead Guilty To Theft Of Trade Secrets From Google

FOR IMMEDIATE RELEASE Wednesday, April 22, 2020

Utah U.S. Attorney Highlights DOJ China Initiative During Remarks At Salt Lake City Security Webinar

"About 80 percent of all federal economic espionage prosecutions have conduct that would benefit China and around 60 percent of federal trade secret theft cases have some nexus to China," Huber said.

FOR IMMEDIATE RELEASE Tuesday, March 17, 2020

Iranian National Extradited to the Western District of Texas for Illegally Exporting Military Sensitive Items from the U.S. to Iran

FOR IMMEDIATE RELEASE Thursday, February 27, 2020

Chinese National Sentenced for Stealing Trade Secrets Worth $1 Billion

China is targeting everything from agricultural techniques to medical devices

- "They've pioneered an expansive approach to stealing innovation through a wide range of actors,"
- Wray told the audience that China is targeting everything from agricultural techniques to medical devices in its efforts to get ahead economically. While this is sometimes done legally, such as through company acquisitions, China often takes illegal approaches, including cyber intrusions and corporate espionage.

> **"They've shown that they're willing to steal their way up the economic ladder at our expense."**
>
> FBI Director Christopher Wray

Just last month, a Harvard University professor was charged with lying about his contractual arrangement with China.

https://www.fbi.gov/news/stories/wray-addresses-china-threat-at-doj-conference-020620
https://www.fbi.gov/news/speeches/responding-effectively-to-the-chinese-economic-espionage-threat

Information is a powerful driver!

Copied from http://www.agriculture.com/news/business/chinese-nationals-charged-with-stealing_5-ar36216

There can be other interests as well

Copied from http://www.wsj.com/articles/u-s-steel-accuses-china-of-hacking-1461859201

Something to watch (possible driver)

02/07/2019

Evolving Made in China 2025

China's industrial policy in the quest for global tech leadership

Four years ago, China launched its ambitious industrial strategy Made in China 2025 and caused considerable irritation around the world. The blueprint for China's path to becoming an industrial superpower has changed the way foreign companies, business associations, and governments view the country. They increasingly perceive the People's Republic more as a systemic rival than a partner. Made in China 2025 has recently disappeared from official rhetoric of the Chinese leadership. But Beijing's aims remain unchanged and its industrial policy is already being implemented: it wants Chinese companies to become global leaders in ten core industries by 2025. And it aims to be a global technological superpower by 2049.

https://www.merics.org/en/papers-on-china/evolving-made-in-china-2025

Another edge of the Coronavirus

VOICE

China Is Bargain Hunting—and Western Security Is at Risk

Beijing could use the coronavirus-induced economic crisis to go on a buying spree. The U.S. and European governments must restrict the purchasing of distressed companies in sensitive sectors.

BY ELISABETH BRAW | APRIL 15, 2020, 3:55 PM

https://foreignpolicy.com/2020/04/15/china-is-bargain-hunting-and-western-security-is-at-risk/

Coronavirus- impact

DoD Must Brace For Long-Term Supply Chain Problems; Big Mergers Likely

"The impact of the COVID crisis in the aviation sector has been really nothing short of catastrophic," said Hunter. "At this point, it's very challenging for those companies to stay in business."

https://breakingdefense.com/2020/04/dod-must-brace-for-long-term-supply-chain-problems-big-mergers-likely/?

Defense News ---- May 22, 2018

Pentagon

The US is running out of bombs — and it may soon struggle to make more

Overall, the authors found that of the 121 second-tier suppliers for munition capabilities, 98 percent of them were single/sole source. And of the 73 third-tier suppliers, 98 percent were also single/sole source.

…"key suppliers are foreign-owned, with no indigenous capability to produce vital parts and materials — setting up the risk that a conflict with China could rely on Chinese-made parts. "

https://www.defensenews.com/pentagon/2018/05/22/the-us-is-running-out-of-bombs-and-it-may-soon-struggle-to-make-more/?utm_source=Sailthru&utm_medium=email&utm_campaign=ebb-5-23&utm_term=Editorial%20-%20Military%20-%20Early%20Bird%20Brief

Modes

- Acquisition
- Cyber
- Investment
- Joint-Venture
- Recruitment
- Theft
- Well-intentioned assistance

knowingly benefit any foreign government, foreign instrumentality, or foreign agent

Awareness and good procedures are needed

5-Year-Long Cyber Espionage Campaign Hid in Google Play

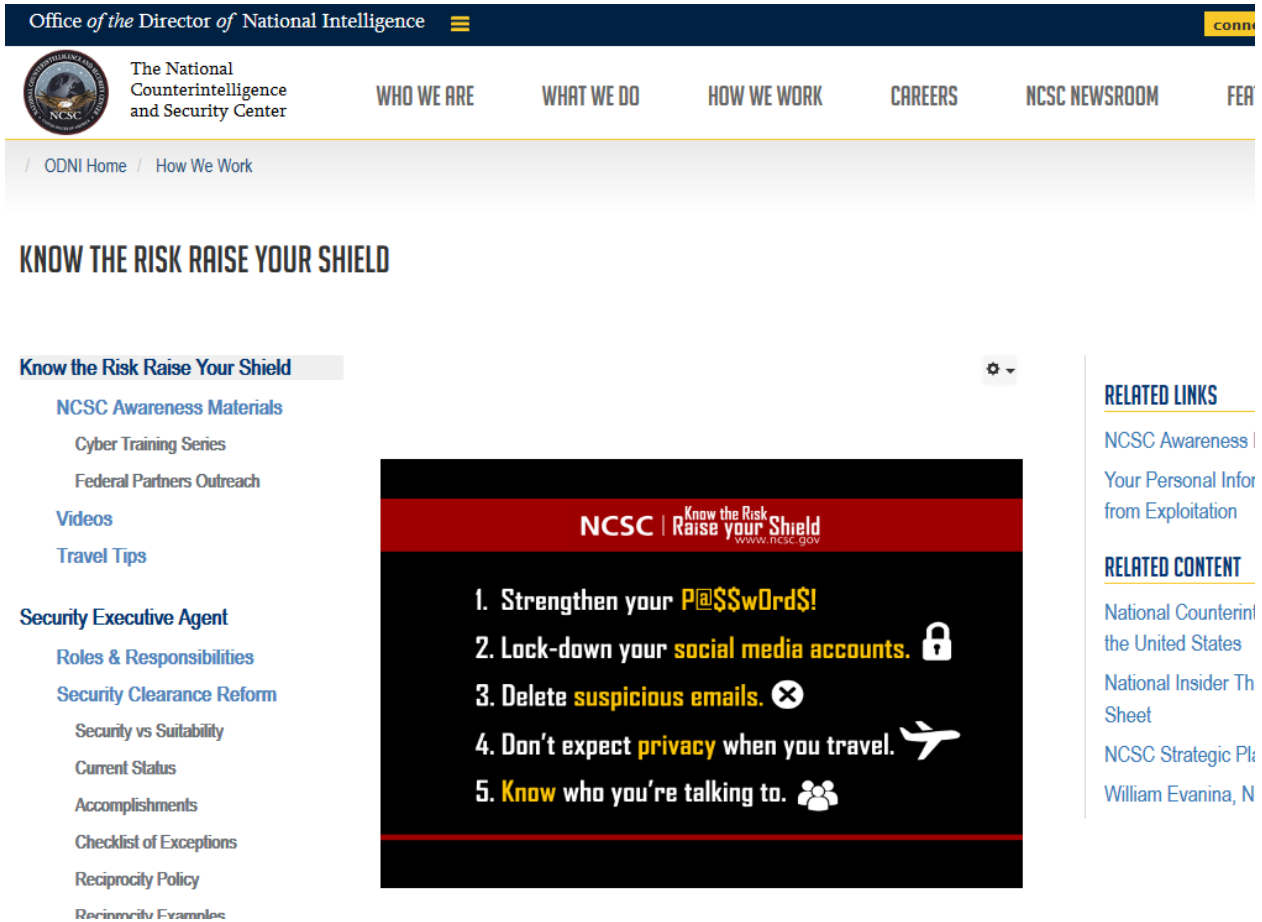
OceanLotus targeted Android devices in the so-called PhantomLance campaign.

A targeted cyber-spying mission waged by a notorious hacking team out of Vietnam preyed mainly on Android users in Southeast Asia and evaded detection in Google Play, APKpure, and other app markets for five years.

Researchers at Kaspersky today revealed details of their study of the attack campaign they call PhantomLance, which they believe is the handiwork of OceanLotus. While Kaspersky has a policy of not tying attack groups with specific nation-states, OceanLotus long has been believed to be a Vietnamese advanced persistent threat (APT) group. PhantomLance — which targets Android — has managed to stay alive by changing up its malware along the way to evade detection.

https://www.darkreading.com/endpoint/5-year-long-cyber-espionage-campaign-hid-in-google-play/d/d-id/1337676?

Know the Risk Raise Your Shield - DNI



https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield

Awareness is key!

- Not just occasional awareness –
- Routine awareness!, it's a mindset – situational awareness
- It's also about information, sharing and training.


Social Media Deception

Social Engineering


Spear phishing 2017

Spear Phishing (30 second trailer)


Spear Phishing Full Video

Social Media Deception Trailer

Social Media Deception Full Video

Travel Awareness

Human Targeting

Supply Chain Risk Management

https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield/ncsc-awareness-materials

Economic Espionage – possible indicators

KNOW THE SIGNS

- Working odd hours without authorization
- Taking proprietary information home without authorization
- Unnecessarily copying material
- Disregarding company policies on personal software and hardware
- Accessing restricted websites
- Downloading confidential material
- Conducting unauthorized research

PERSONAL BEHAVIORS

- Unexplained short trips to foreign countries
- Engaging in suspicious personal contacts with competitors, business partners or unauthorized individuals
- Buying items they normally cannot afford
- Overwhelmed by life crises or career disappointments
- Showing concern about being investigated

COMMON FACTORS

- Financial need
- Greed
- Unhappiness in the workplace
- Different allegiances to another company or country
- Drug/Alcohol abuse
- Vulnerability to blackmail
- Job offers from other organizations

https://www.fbi.gov/file-repository/economic-espionage-508.pdf/view

Identify Information sources

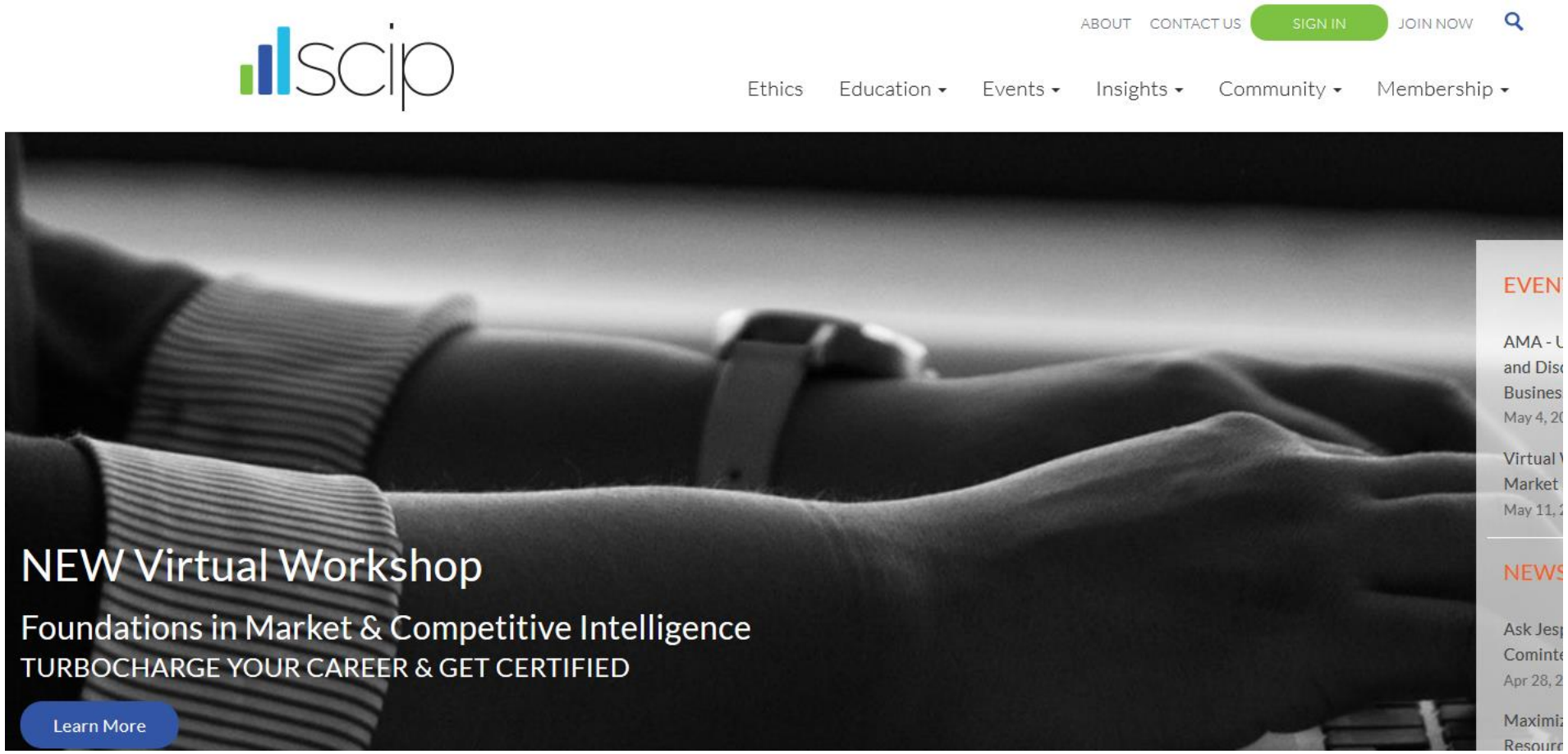
- Staff
- Staff interactions
  - Family
  - Friends
  - Colleagues
  - Events
- Visitors
- Prospective customers
- Facility visits tours
- Garbage | Recycling | Scrap | “bone yard – equipment” | legacy items “always been”
- Web
- Press Releases
- Signature Block information – too much (details)

Review sources | Identify potential issues

- As the question(s)
  - How would I access information?
  - What can I learn just by being observant?
  - If I wanted to – I could do _____
  - Actively learn –
    - What do I know about Social Engineering?
    - What do I know about Competitive Intelligence procedures?
    - How do we look at and review – normal and seemingly uninteresting processes?
    - What information do we handle and/or possess?

Be aware of transition points

Identify possible resources



https://www.scip.org/default.aspx

Identify possible resources & validate

Member Advisory Board

As a non-profit, SCIP is governed by a Member Advisory Board (and bylaws) that sets the strategy and ensures that the members are at the center of every decision we make.

CHAIR - Paul Santilli
Hewlett Packard Enterprise

Maureen Nail
Pfizer

Jay Nakagawa
Dell Technologies

Ellie Mirman
Crayon

https://www.scip.org/page/About-Us

One technique - Elicitation

- Elicitation is a technique used to collect information that is not readily available and do so without raising suspicion that specific facts are being sought.
- Elicitation is not rare –
  - “It is not uncommon for people to discover information about a person without letting on the purpose.
  - **For example**, have you ever planned a surprise part for suomeone and needed to know their schedule, wish list, food likes and silike aor other information without that person finding out your were collectingthe information or for what purpose?
  - The problem is when a skilled elicitor is able to obtain valuable information from you, which you did not intend to share because you did not recognize and divert the elicitation.

https://www.fbi.gov/file-repository/elicitation-brochure.pdf/view

Elicitation – some techniques

- Assumed Knowledge
- Bracketing
- Can you top this?
- Confidential Bait
- Criticism
- Deliberate False Statements/Denial of the Obvious
- Feigned Ignorance
- Flattery
- Others

https://www.fbi.gov/file-repository/elicitation-brochure.pdf/view

Red Flag Questions

1. Buyer is reluctant to offer information about the end-use of the ordered product
2. Product's capabilities do not fit the buyer's line of business
3. Buyer's IP address does not match the stated location
4. Company receives the same request for a quote (RFQ) from multiple customers
5. The RFQ appears to be cut-and-pasted into the email
6. Buyer carbon copies unknown individuals
7. A freight forwarder, Importer/ Exporter, or General Trading Company is listed as the final
8. Routine installation, training, warranty, or maintenance services are declined by the buyer
9. Buyer is unfamiliar with the product’s performance.
10. Buyer is evasive when asked about whether parts are for domestic use or re-export
11. Buyer has little to no presence on the Internet
12. The shipping address is a residence or a building that leases virtual office space
13. Unusual method of payment or unexpected source of payment

https://www.fbi.gov/video-repository/made-in-america-092019.mp4/view

Historical Examples

- Maps – trade routes, routes to …
- Skills/craftsmen – English skilled craftsmen
- Technology - cotton gin – thread, others

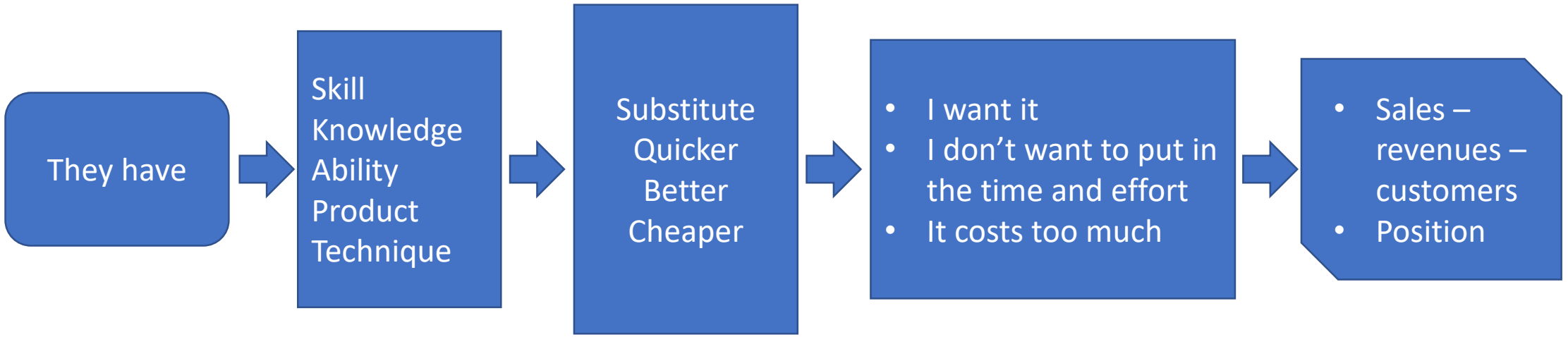
Drivers

- Peer recognition
- Economic viability
- Product duplication
- Strategic positioning/capability

What is being sought?

- Information that will contribute to benefits from being able to do things –
  - Faster
  - Better
  - Cheaper
  - Identical substitute

Driving equation



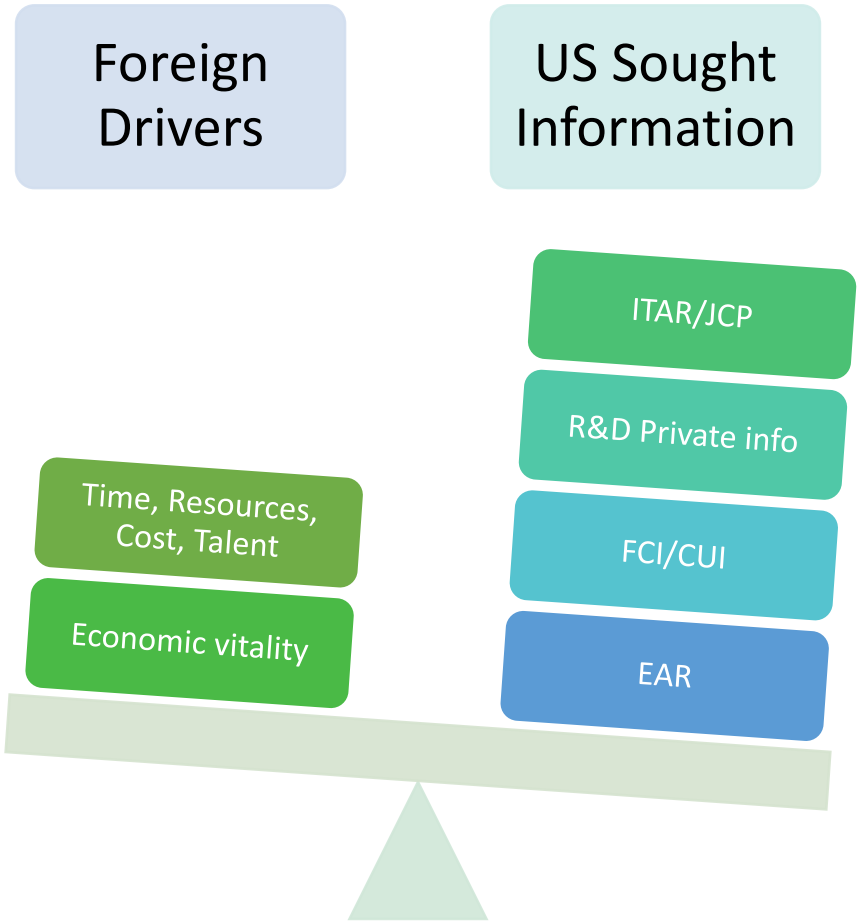
How one can gain the upper hand?

- Time
- Time and Effort
- Time, effort, investment

Costly, Difficult, Involved – no guaranteed outcome

- Partnering – teaming – joint ventures
- Licensing – non-compete clauses, etc

Seeking Parity



"As you all know, foreign governments and other non-state adversaries of the United States are engaged in an aggressive campaign to evade U.S. sanctions regimes and acquire sensitive U.S. technology. In so doing, they threaten our economy, our prosperity and, most importantly, our national security. Disrupting these national security threats is among the highest priorities of the Department of Justice, and the National Security Division."

"Because our companies have our nation's crown jewels in their possession. They house information targeted by thieves ranging from foreign powers bent on economic and military superiority, to individual criminals who know the market demand for this information, to terrorists who wish to create weapons of mass destruction."

Assistant Attorney General John P. Carlin Delivers Remarks at Practising Law Institute's Coping with U.S. Export Controls and Sanctions 2015 Conference, Washington, DC, United States -Friday, December 18, 2015

"Penetrating and influencing the US national decision making apparatus and Intelligence Community will remain primary objectives for numerous foreign intelligence entities. Additionally, the targeting of national security information and proprietary information from US companies and research institutions involved with defense, energy, finance, dual-use technology, and other sensitive areas will remain a persistent threat to US interests."

STATEMENT FOR THE RECORD WORLDWIDE THREAT ASSESSMENT of the US INTELLIGENCE COMMUNITY February 9, 2016 – page 10

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Friday, January 29, 2016

U.S. Navy Officer Sentenced to 40 Months in Prison for Selling Classified Ship Schedules as Part of Navy Bribery Probe

A U.S. Navy Lieutenant Commander was sentenced today to 40 months in prison for accepting cash, hotel expenses and the services of a prostitute from foreign defense contractor Glenn Defense Marine Asia (GDMA) in exchange for classified U.S. Navy ship and submarine schedules and other internal Navy information.

Department of Justice

U.S. Attorney's Office

Southern District of New York

FOR IMMEDIATE RELEASE

Thursday, April 14, 2016

Manhattan U.S. Attorney Announces Arrest Of Chinese National For Illegally Attempting To Export High-Grade Carbon Fiber To China

Department of Justice

United States Attorney Channing D. Phillips
District of Columbia

FOR IMMEDIATE RELEASE
Monday, April 4, 2016
WWW.JUSTICE.GOV/USAO/DC

CONTACT: BILL MILLER
202-252-6933

SINGAPORE MAN EXTRADITED TO UNITED STATES IN CONNECTION WITH PLOT INVOLVING EXPORTS TO IRAN OF U.S. COMPONENTS LATER FOUND IN BOMBS IN IRAQ


Domestic Security Partnership
Protecting the Nation Through Trusted Partnerships and Enhanced Security

OUR MISSION

CREATING A MORE SECURE AMERICA THROUGH PUBLIC/PRIVATE PARTNERSHIPS

The Domestic Security Partnership seeks to strengthen United States security by fostering collaboration and cooperation among governmental and private sector security professionals. The DSP achieves its mission by supporting the Domestic Security Alliance Council through engagement, education symposia, and security information exchange.

The National Cyber-Forensics and Training Alliance (NCFTA) was established in 2002 as a nonprofit partnership between private industry, government, and academia for the sole purpose of providing a neutral, trusted environment that enables two-way collaboration and cooperation to identify, mitigate, and disrupt cyber crime.

Our focus is on results. By combining shared information and making the resulting intelligence actionable, the NCFTA has enabled our community of trusted partners to prevent over $1 billion in potential losses while also helping to identify critical threats impacting private industry and supporting global law enforcement by helping to identify current threats most impactful to industry.

$2.39 Billion	15,187	1,666	1,096
Financial losses prevented	Intelligence reports produced	Cases referred to law enforcement	Law enforcement arrests

https://www.ncfta.net/

U.S. Department of Justice

Robert L. Capers
United States Attorney
Eastern District of New York

271 Cadman Plaza East
Brooklyn, New York 11201

FOR IMMEDIATE RELEASE

March 1, 2016

Contact:
Nellin McIntosh
United States Attorney's Office
(718) 254-6323

PRESS RELEASE

CHIEF EXECUTIVE OFFICER OF INTERNATIONAL METALLURGICAL COMPANY ARRESTED FOR EXPORTING AEROSPACE-GRADE METALS TO IRAN

Defendant Exported High-Tech Material Used in Missile Production and Nuclear Applications

COUNTERINTELLIGENCE

"Insiders who disclose sensitive US Government information without authorization will remain a significant threat in 2016. The sophistication and availability of information technology that can be used for nefarious purposes exacerbate this threat both in terms of speed and scope of impact."

Former Connecticut Resident Sentenced to Over Eight Years in Prison for Attempting to Send U.S. Military Technology to Iran

Mozaffar Khazaee, 61, formerly of Manchester, Connecticut, was sentenced today to 97 months in prison and ordered to pay a $50,000 fine by U.S. District Judge Vanessa L. Bryant of the District of Connecticut for violating the Arms Export Control Act by attempting to send to Iran highly sensitive, proprietary, trade secret and export controlled material relating to U.S. military jet engines, which he had stolen from multiple U.S. defense contractors where he had previously been employed.

Assistant Attorney General for National Security John P. Carlin, U.S. Attorney Deirdre M. Daly of the District of Connecticut, Special Agent in Charge Matthew Etre of U.S. Immigration and Customs Enforcement-Homeland Security Investigations (ICE-HSI) Boston, Assistant Director Randall C. Coleman of the FBI's Counterintelligence Division, Special Agent in Charge Craig W. Rupert of the Defense Criminal Investigative Service (DCIS) Northeast Field Office, Special Agent in Charge Danielle Angley of the Air Force Office of Special Investigations and Special Agent in Charge John McKenna of the Department of Commerce's Office of Export Enforcement Boston Office made the announcement.

"Mozaffar Khazaee exploited his privileged access to national security assets to steal highly sensitive military technology with the intent of providing it to Iran," said Assistant Attorney General Carlin. "Violations of the Arms Export Control Act, particularly those involving attempts to transfer sensitive defense technology to a foreign power, are among the most significant national security threats we face, and we will continue to leverage the criminal justice system to prevent, confront, and disrupt them."

May 4, 2018

State Department Announces Another Major ITAR Enforcement Case and $30 Million Penalty

- Failure to apply for and manage export licenses;
- Failure to comply with terms, conditions and provisos of licenses;
- Poor management of use of license exemptions;
- Inaccurate or incomplete shipping documents;
- Improper actions at trade shows;
- Failure to obtain Nontransfer and Use Certificates;
- Failure to properly decrement or report quantities of items shipped;
- Failure to properly record shipments;
- Failure to return items to the U.S. under temporary export licenses;
- Failure to file reports of payments of contributions, fees and sales commissions as required under 22 CFR Part 130;
- Multiple recordkeeping violations.

https://www.jdsupra.com/legalnews/state-department-announces-another-62908/

Feds say Minnesota firm was tricked into illegal shipment of technology to Iran

By STEPHEN MONTEMAYOR | Star Tribune (Minneapolis) | Published: September 2, 2017

MINNEAPOLIS (Tribune News Service) — A Minnesota company was duped into exporting sensitive technology that wound up being shipped to Iran in violation of U.S. export controls, according to a recently unsealed federal indictment.

The indictment names a Malaysian company and two former employees, accusing them of shipping the components to an Iranian firm with close ties to the Iranian government.

The indictment doesn't name the Minnesota company, but a subsequent court filing includes a screenshot of an e-mail addressed to Thief River Falls-based Digi-Key, a large distributor of electronic components such as capacitors, oscillators and integrated circuits.

According to the charges, the company believed it was sending digital communications equipment to "Green Wave Telecommunication, Sdn Bhn" in Kuala Lumpur, Malaysia. But Green Wave later sent the devices to Iran in violation of export controls that cite "national security and anti-terrorism reasons," according to the indictment.

The devices appear to be "dual use" technology, which can be used in civilian products or in weapons guidance systems that would fall under international export controls.

Prosecutors also charged Alireza Jalali, Green Wave's former head of purchasing, and Negar Ghodskani, a woman who simultaneously worked for Green Wave and the Iranian recipient of the technology at the time of the alleged conspiracy.

It is interesting to note that the Minnesota firm – Digi-Key is not a small business. It has been involved in federal procurement since roughly 2003, has approximately 2,600 employees, $1.4B in annual revenue and is listed as an OTSB.

http://www.startribune.com/feds-say-minnesota-firm-was-tricked-into-illegal-shipment-of-technology-to-iran/442520733//

National Intellectual Property Rights Coordination Center

- The mission of the NIPRCC is to ensure national security by protecting the public's health and safety, the U.S. economy, and our war fighters, and to stop predatory and unfair trade practices that threaten the global economy.
- Initiatives
  - **Operation Chain Reaction**
    - targets counterfeit goods entering the supply chains of the Department of Defense (DoD)
  - **Operation Apothecary**
    - targets the growing problem of Internet crime – emphasis on prescriptions/pharmaceuticals
  - **Operation Engine Newity**
    - countering the threat of counterfeit automotive, aerospace, rail, and heavy industry related components that are illegally imported and distributed throughout the United States.

Domestic Security Alliance Council

FBI · Private Industry · DHS · Networking for Security

Home | Policy | Contact Us Search...

HOME | ABOUT | PARTNERS | CONTACTS | TOPICS | PRODUCTS | EVENTS | GET INVOLVED | PORTAL LOG IN

The Domestic Security Alliance Council (DSAC) is a strategic partnership between the U.S. government and the U.S. private industry that enhances communication and promotes the timely and effective exchange of security and intelligence information between the federal government and the private sector.

Insider Threat

- **The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy (FBI)**

This brochure serves as an introduction for managers and security personnel on how to detect an insider threat and provides tips on how to safeguard your company's trade secrets.

- **Economic Espionage: How to Spot a Possible Insider Threat (FBI, May 2012)**

This article talks about the threat of corporate insiders stealing secrets, focusing on foreign economic espionage. It includes cases examples and potential warning signs.

- **Combating the Insider Threat (DHS National Cybersecurity and Communications Integration Center, May 2014)**

This document includes characteristics of insiders at risk of becoming a threat, behavioral indicators of malicious threat activity, behavioral prediction theories, countermeasures and deterrence methods, and training suggestions.

- **National Counterintelligence and Security Center Insider Threat Webpage**

This webpage contains link to relevant documents and websites.

Filed under: Frontpage Feature

https://www.dsac.gov/topics/insider-threat

Good videos

Economic Espionage

- **FBI Launches Nationwide Awareness Campaign**

- The Company Man: Protecting America' Secrets
  https://www.fbi.gov/news/stories/economic-espionage
- Made in America
  - https://www.fbi.gov/video-repository/made-in-america-092019.mp4/view
- GAME OF PAWNS - The Glen Duffie Shriver Story
  - https://www.youtube.com/watch?v=TEYRLDvJaxo&feature=youtu.be

Resource - video

- **WORLD EXCLUSIVE: Chinese spy spills secrets to expose Communist espionage | 60 Minutes Australia**
  - https://www.youtube.com/watch?v=zdR-I35Ladk