Counterintelligence Awareness, Reporting, and Partnership Briefing

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Larry Hite

This brief has been produced by the Defense Counterintelligence and Security Agency (DCSA) for DoD Contractors and Government Agencies as Part of their security program. Questions and requests to further distribute this publication should be addresses to the DCSA Directorate of Counterintelligence

WARNING: This report may contain information with United States Persons as defined by Executive Order 12333 and Department of Defense Manual 5240.01. Such Information should be handled and protected in accordance with applicable Intelligence Oversight rules by persons and organizations subject to those rules. DCSA collects, retains, and disseminates United States Persons information with all applicable laws, directives, and policies. Should you require minimized USPI, c

Introduction

- Insert CDSE CI Awareness video here and delete this bullet (See notes for instructions on how to add the video file)

Agenda

- DCSA Authorities
- What is Counterintelligence (CI)?
- Industry Reporting
- Methods of Contact
- Insider Threat
- Cyber / Social Networking

Who Are We? – DCSA Authorities

- DoDD 5105.42
  - Establishes DCSA as a Defense Agency under the authority, direction, and control of the Under Secretary of Defense for Intelligence (USD(I))
  - Identifies DCSA as the DoD Cognizant Security Agency for Industrial Security
  - Directs DCSA to manage & administer the DoD portion of the National Industrial Security Program (NISP) for the DoD and 24 other U.S. departments/agencies

- DoDI 5240.19
  - Outlines DCSA's responsibility to conduct CI activity within the Defense Industrial Base (DIB) in areas of security, threats, suspicious incidents, and countermeasure implementation

What is Counterintelligence?

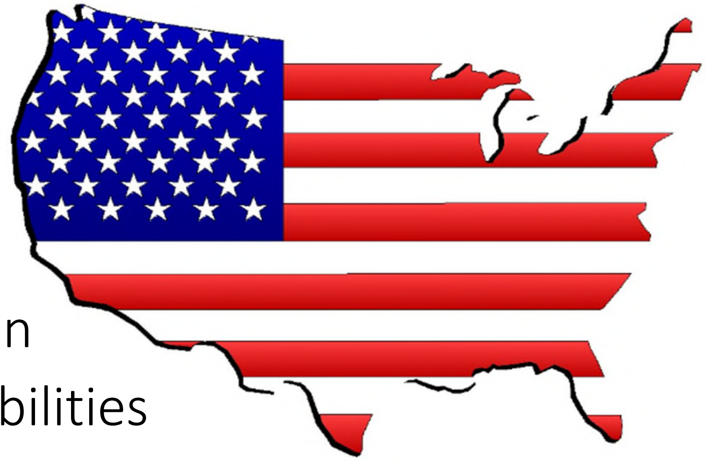
- Information gathered and activities conducted to protect against:
  - Espionage
  - Sabotage
  - Assassinations
  - Other intelligence activities

- Conducted by or on behalf of…
  - Foreign governments or elements thereof
  - Foreign organizations
  - Foreign persons
  - International terrorist organizations

President Truman signing the National Security Act of 1947

What Should We Protect?

Any information that would degrade the nation's advantage if compromised



- Protect anything that may:
  - Damage national security
  - Alter program direction, scope, or duration
  - Compromise the program or system capabilities
  - Shorten the expected system life
  - Deals with Critical Technology in order to counter the impact of loss

It does NOT always involve classified information!

Industry Reporting

- If You Have to Say “NO,” let DCSA know
  - If asked for proprietary information
  - If asked for export controlled items
  - If asked for classified information
  - If asked for dual use technology (military/commercial use)
  - If asked for technology outside requestor’s scope of business
  - If solicitor is acting as procurement agent for foreign government
  - If the request is unusual, etc.
  - Any anomalies

Industry Reporting Requirements

DoD 5220.22-M (NISPOM)

- 1-301: Terrorism, Subversion, Espionage, Sabotage; Reports to be submitted to the FBI & CSA
- 1-302a: Adverse Information: Report adverse information to CSA
- 1-302b: Suspicious Contacts: Report efforts to obtain illegal/unauthorized access to classified information or to compromise a cleared employee
- 1-303: Reports of loss, compromise, or suspected compromise: Security Violations

DCSA Industrial Security Letter 2010-02 & 2013-05

Reporting Requirements for Cyber Intrusions

Contractor Reporting of Potential Espionage Indicators (PEI)

- NISPOM Guidance:
  - 1-302 a. Adverse Information.
    - Contractors shall report adverse information coming to their attention concerning any of their cleared employees.
    - Reports based on rumor or innuendo should not be made.
    - The subsequent termination of employment of an employee does not obviate the requirement to submit this report.
    - If the individual is employed on a Federal installation, the contractor shall furnish a copy of the report and its final disposition to the commander or head of the installation.
- Becker vs. Philco and Taglia vs. Philco (389 U.S. 979):
  - The U.S. Court of Appeals for the 4th Circuit decided on February 6, 1967, that a contractor is not liable for defamation of an employee because of reports made to the government under requirements of this manual and its previous versions.

What are the Trends in Industry

Targeting U.S. Technologies

A Report of Foreign Targeting of Cleared Industry

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

2019

Insert the video file here

Targeting U.S. Technology Summary

Most Targeted Technologies

Electronics

Aeronautic Systems

Command, Control, Communication, & Computers (C4)

Armament & Survivability

Optics

Radars

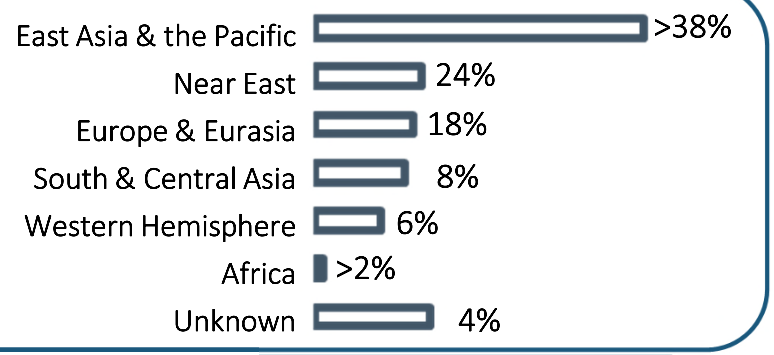
Software

Space Systems

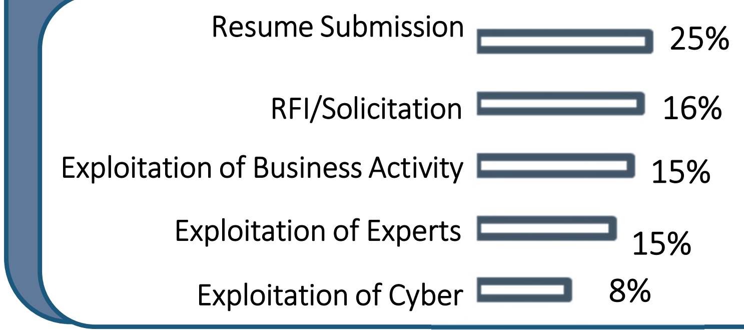
Marine Systems

Energy Systems

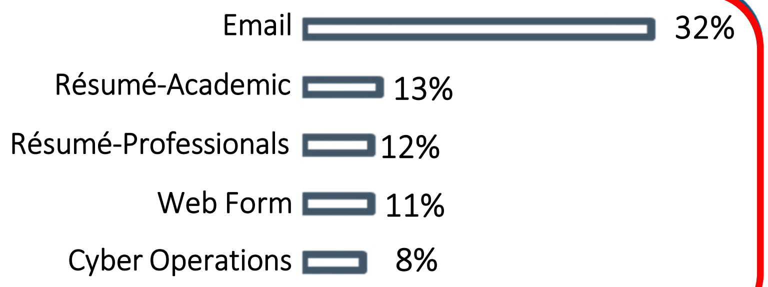
Targeting by Geographic Region 2024



Top Five Methods of Operation 2024



Top Five Methods of Contact 2024



Case Study

- In May 2023, a representative from a Europe and Eurasia space agency sent an unsolicited email to a CC requesting information on the detection of damage and spinning rate analysis for a satellite in Low Earth Orbit. The CC specializes in development/application of AI capabilities to enhance real-time sensor data utilization. Gaining access to U.S. satellite damage and spinning rate data can advance foreign space technology in increasing low orbit satellite lifespan and functionality, allowing longer influence in lower orbit space

Target Areas

- Overseas Travelers (pre-brief & debrief)
  - Employees more vulnerable to foreign collection attempts outside the United States
- Hosting Foreign Visits
  - Primary contact with visiting foreigners; arranging the visit; prime elicitation target
- Business Development Personnel
  - Virtue of duties make them first-contact for business proposals
- Sales / International Sales
  - Initial contact; continued contact; website / web-form requests; low cost, high gain targeting
- Human Resource Personnel
  - Employment often sought to get close to classified programs; resumes

Target Areas (Cont.)

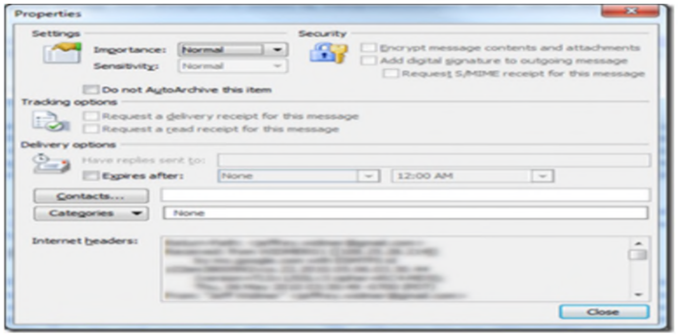
- Gate Keepers (Admin Assistants/Receptionists)
  - Familiarity with inner workings make for ideal foreign targeting
- Technology (IT) Personnel
  - Best positioned to discern cyber attacks (from inside or outside)
- Published researchers, scientists, engineers, etc.
  - Specifically targeted for exploitation by hostile services
- Public Affairs Personnel
  - Typically knowledgeable of foreign visitors or requests for info

Identifying Suspicious Contacts

- Emails
- Phone Calls / Fax / Web-requests
- Elicitation
- Foreign Visits
- Foreign Travel
- Conferences / Symposiums / Trade Shows

Emails/RFIs

- Possible Indicators
  - Email/Internet addresses from a foreign country
  - Recipient uses only a personal address and will not provide a business or government email address
  - It is unknown how they got your email address
  - Technology requested is classified, export-controlled, or dual-use
  - Requester is a student, consultant, or employee of a foreign government
  - Requester will not divulge end-user
  - Recipient is told not to worry about security concerns



Properties

Settings

Importance: Normal

Sensitivity: Normal

□ Do not AutoArchive this item

Security

□ Encrypt message contents and attachments

□ Add digital signature to outgoing message

□ Request S/MIME receipt for this message

Tracking options

□ Request a delivery receipt for this message

□ Request a read receipt for this message

Delivery options

Have replies sent to:

□ Expires after: None 12:00 AM

Contacts...

Categories None

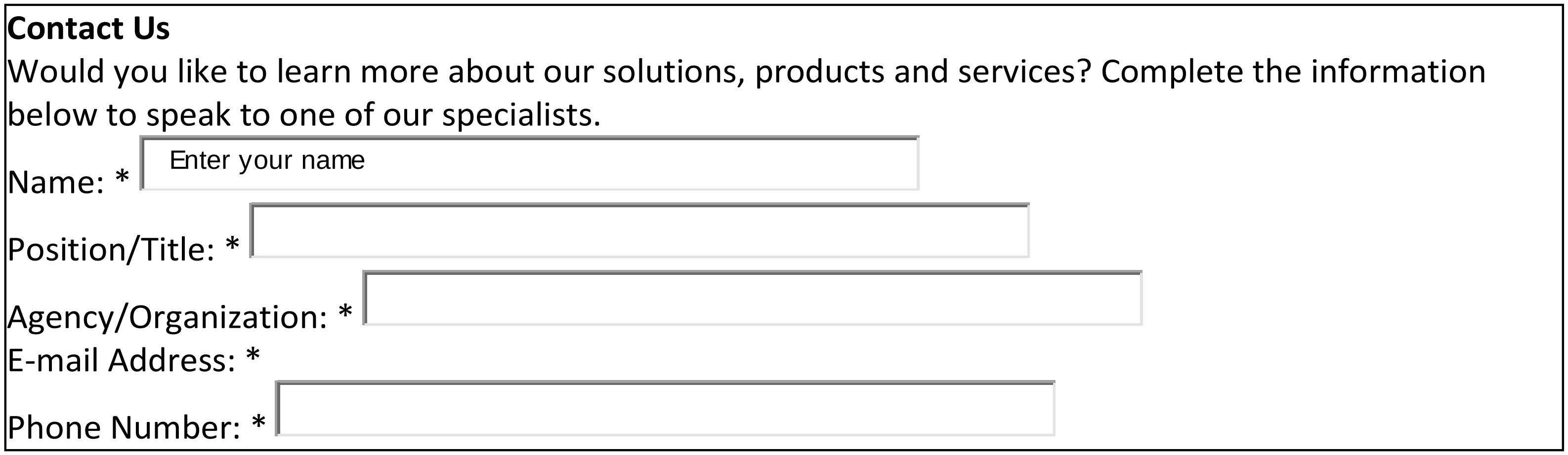
Internet headers: [redacted]

Close

Expand header/footer information:
(Outlook) Open email>>File>>Properties>>Copy Headers

Website Contact Us Form

- Possible Indicators
  - Contact information is from a foreign country
  - Technology requested is classified, export-controlled, or dual-use
  - Claims to be a student, consultant, employee of a foreign government
  - Requester will not divulge end-user
  - Assures the sales team that export licenses are not required
  - Employee is told not to worry about security concerns
  - Web-form, or “Contact Us” form, easy way to make contact



Contact Us

Would you like to learn more about our solutions, products and services? Complete the information below to speak to one of our specialists.

Name: * Enter your name

Position/Title: *

Agency/Organization: *

E-mail Address: *

Phone Number: *

Elicitation

- Elicitation (or social engineering) is the subtle extraction of information during an apparently normal and innocent conversation
- Conducted by a skilled intelligence collector can appear to be a social or professional conversation and can occur anywhere (restaurant, conference, or one's home)

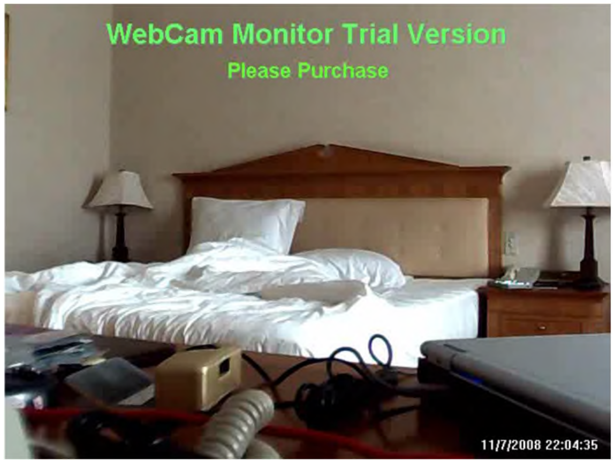
- Foreign Intelligence Entities are very patient and skilled
- Don't answer questions outside your scope
  (Stay in your lane)
- Answer a question with a question
  (Why are you asking me this?)

Foreign Visits

- Possible Indicators
  - Peppering & questions outside the scope of the approved visit
  - Wandering or distraught visitor who acts offended when confronted
  - Divide and conquer technique to separate from group
  - Switch visitors: Last minute additions or changes to the visit
  - Bait and switch: Changing the scope of the visit at the last minute
  - Prohibited Electronics: Bringing phones / cameras / video into areas where none are allowed
  - Visitors who conceal their foreign government ties

- Know your Technology Control Plan (TCP)
- Consider a visitor cell phone policy
- Name checks prior to the visit
- Business Cards

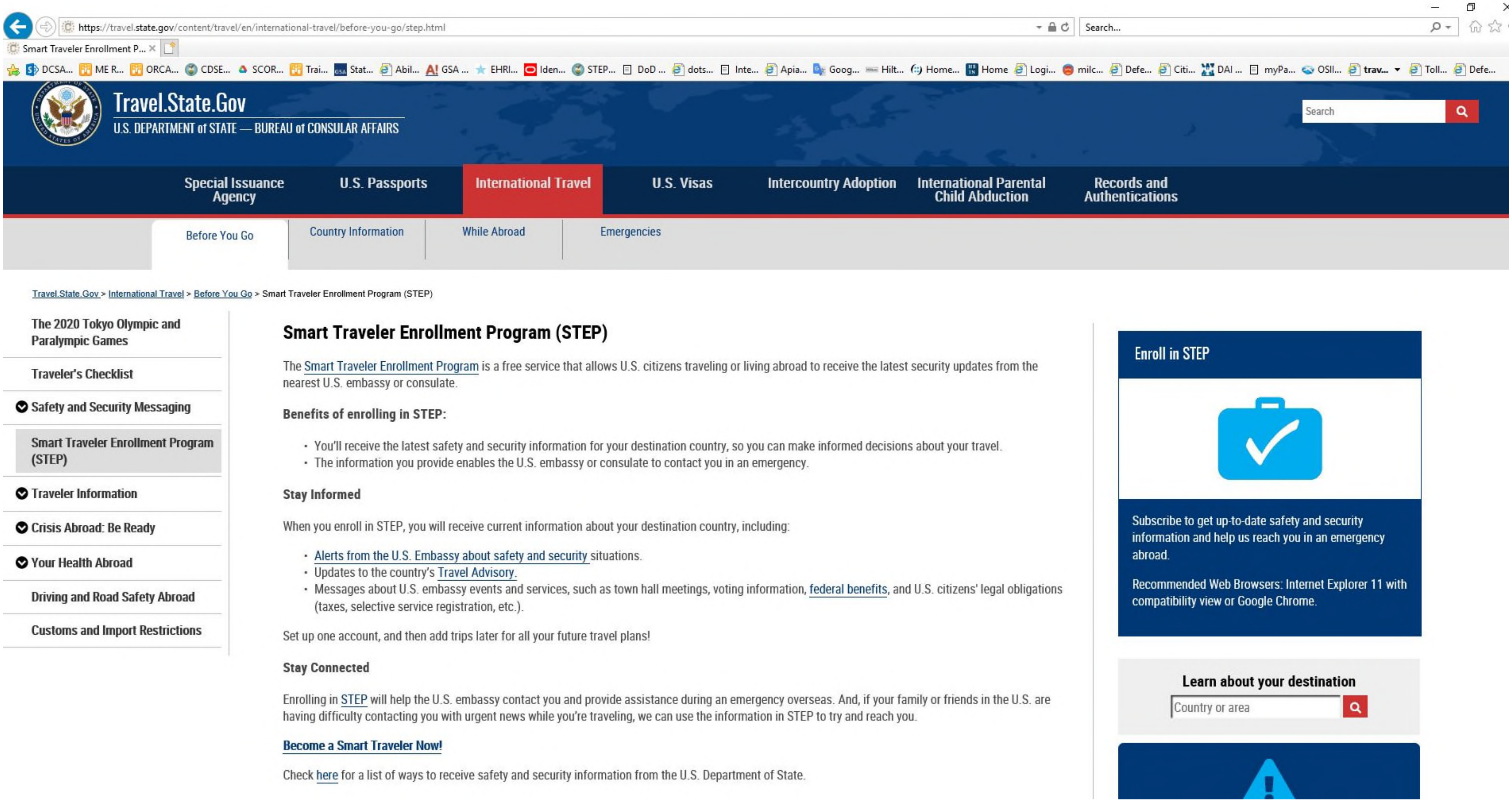
Foreign Travel



- Possible Indicators
  - Hotel room seems as if it was searched
  - Theft
  - The appearance of being followed
- Countermeasures
  - Leave unnecessary devices at work / home
  - Use a travel laptop or removable hard-drive
  - Computer scans before leave / upon return
  - Don’t publicize travel plans (social media)
  - Pre / Post travel security briefings

- Do you need to take your laptop?
- Computer scans before leave / upon return
- Business Cards

Foreign Travel (Cont.)


https://travel.state.gov/content/travel/en/international-travel/before-you-go/step.html
Search...
Smart Traveler Enrollment P...
DCSA... ME R... ORCA... CDSE... SCOR... Trai... Stat... Abil... GSA ... EHRI... Iden... STEP... DoD ... dots... Inte... Apia... Goog... Hilt... Home... Home Logi... milc... Defe... Citi... DAI ... myPa... OSII... trav... Toll... Defe...
Travel.State.Gov
U.S. DEPARTMENT of STATE — BUREAU of CONSULAR AFFAIRS
Search
Special Issuance Agency
U.S. Passports
International Travel
U.S. Visas
Intercountry Adoption
International Parental Child Abduction
Records and Authentications
Before You Go
Country Information
While Abroad
Emergencies
Travel.State.Gov > International Travel > Before You Go > Smart Traveler Enrollment Program (STEP)
The 2020 Tokyo Olympic and Paralympic Games
Traveler's Checklist
Safety and Security Messaging
Smart Traveler Enrollment Program (STEP)
Traveler Information
Crisis Abroad: Be Ready
Your Health Abroad
Driving and Road Safety Abroad
Customs and Import Restrictions
Learn about your destination
Country or area

Smart Traveler Enrollment Program (STEP)

The Smart Traveler Enrollment Program is a free service that allows U.S. citizens traveling or living abroad to receive the latest security updates from the nearest U.S. embassy or consulate.

Benefits of enrolling in STEP:

- You'll receive the latest safety and security information for your destination country, so you can make informed decisions about your travel.
- The information you provide enables the U.S. embassy or consulate to contact you in an emergency.

Stay Informed

When you enroll in STEP, you will receive current information about your destination country, including:

- Alerts from the U.S. Embassy about safety and security situations.
- Updates to the country's Travel Advisory.
- Messages about U.S. embassy events and services, such as town hall meetings, voting information, federal benefits, and U.S. citizens' legal obligations (taxes, selective service registration, etc.).

Set up one account, and then add trips later for all your future travel plans!

Stay Connected

Enrolling in STEP will help the U.S. embassy contact you and provide assistance during an emergency overseas. And, if your family or friends in the U.S. are having difficulty contacting you with urgent news while you're traveling, we can use the information in STEP to try and reach you.

Become a Smart Traveler Now!

Check here for a list of ways to receive safety and security information from the U.S. Department of State.

Enroll in STEP

Subscribe to get up-to-date safety and security information and help us reach you in an emergency abroad.

Recommended Web Browsers: Internet Explorer 11 with compatibility view or Google Chrome.

Conferences, Conventions, Trade Shows

Clue = All Expenses Paid

- Possible Indicators
  - Unsolicited invitation to overseas conference or symposium
  - Being approached by individuals who are overly knowledgeable of you and your work
  - Approved guests bringing uninvited participants to the event (known as "shoe horning")
  - Foreigners attempting to access events that are closed to foreigners (feigning ignorance)
  - Suspicious behavior at the CCT (photographs, following an employee, invitations to events, etc.)

Suspicious contact after you return from your trip (Saying, "I met you at the trade show")

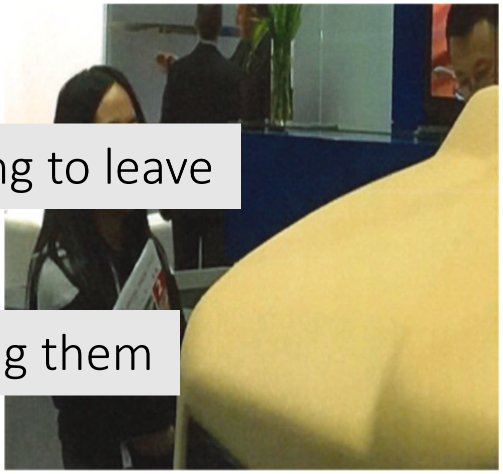
Business cards

Conferences, Conventions, Trade Shows

Suspicious Behaviors

Aggressively inspecting displays or refusing to leave

Questionable badge credentials / hiding them



Asking detailed questions, where answers could reveal controlled information

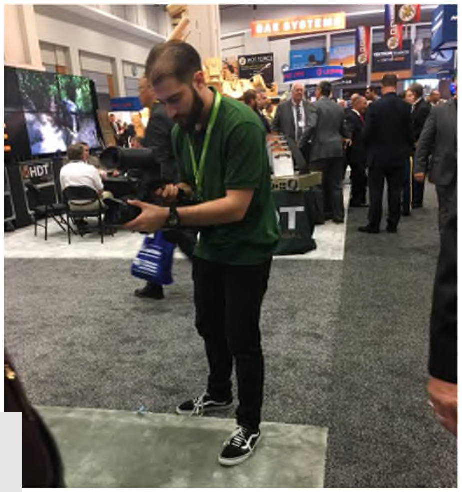
Cre

Social Networking

Business cards

Multiple cell phones or cameras

Swarm tactics



Claiming to be journalists

Exploitation of Relationships

- Joint ventures and joint research may provide opportunities for elicitation and access to employees / networks
- Joint efforts place foreign personnel in close proximity to cleared employees and technology
- Adversaries seek to build rapport and prey on eagerness to develop or expand commercial relationships
- Front companies posing as legitimate businesses

Be wary of providing information beyond the scope of the meeting or business activity

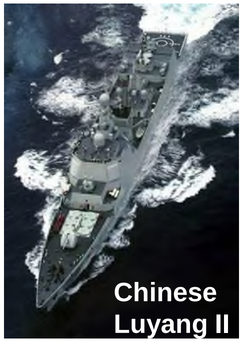
Insider Threat

Most damaging espionage cases were carried out by insiders

- (USPER1) Chi Mak

Secret clearance
L3 Power Paragon
Naval QED propulsion technology
VA class submarine
Aegis battleship
China
24 yrs prison / $50,000

U.S. Aegis battleship


Chinese Luyang II

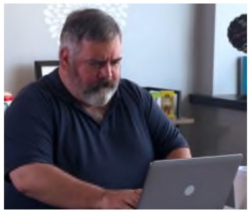
- (USPER2) Greg Bergersen

Secret clearance
Pentagon contractor
Taiwan's air defense system
US plans in Taiwan
China
57 months / 16 yrs prison

Money
Ideology
Compromise
Ego
Revenge

Cyber: Phishing

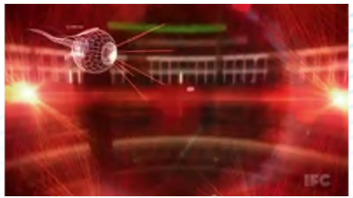
- Socially-engineered email aka “phishing” or “spear-phishing” is the most common method our adversaries use to get inside computer networks



- A socially-engineered email is:
  - An email with maliciously-crafted <u>attachments or links</u> to a malicious website
  - High level of targeting sophistication (spear-phishing)
  - May appear to come from an associate, client, or acquaintance
  - May be contextually relevant to your job

Do not open attachments (or clink on links) from someone you do not know

Cyber / Social Networking



Cyber

- Malicious links or attachments
- Spearphishing
- Spoofed emails
- Un-patched or zero-day vulnerabilities
- Compromised media (USB drives)
- Credential harvesting
- Easily broken passwords
- Attempted and successful intrusions
- Access Controls & User Account Audits
- Review BYOD policies

Social Networking

- Great tool, but…
- False identities, personas
- Vulnerable to spearphishing, spoofing, hacking
- Tremendous volume of users presents targets of opportunity
- Can be used for reconnaissance and elicitation
- Remember NEED-TO-KNOW. Only post what is needed
- Adjust your security settings
- Not everyone is a friend!

Do not open attachments (or clink on links) from someone you do not know

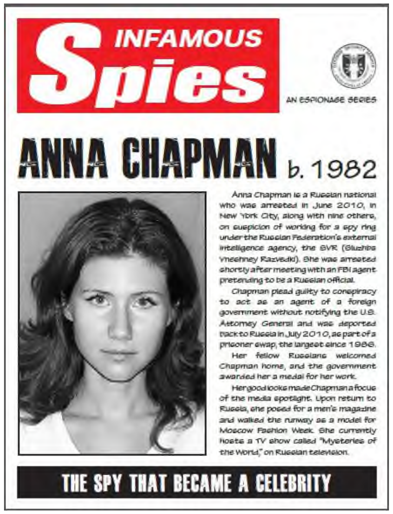
Social Networking Tips

- NEED-TO-KNOW. Only post information that you are comfortable with others knowing
- No detailed biographic information
- Do not list your home address or personal phone number (A phone number can be used to perform a reverse look-up and find your home address)
- Adjust security settings, lock down pictures and personal information
- Do not divulge sensitive company information. Limit project-specific descriptions
- Remember! Not everyone is your friend. Do not blindly accept every business associate, referral, or friend invitation

<u>Never</u> divulge your clearance level or that you work on classified projects

Social Networking: Case Study

- Anna Chapman (Anna Vasilyevna Kushchenko) is the daughter of a Russian Intelligence General
- Anna was a deep cover Russian intelligence officer targeting U.S. policy, economics, and personnel who had access
- Anna used a popular social networking site to socially engineer her targets and later used Steganography to hide (encrypt) her emails back to Russia



INFAMOUS Spies

AN ESPIONAGE SERIES

ANNA CHAPMAN b. 1982

Anna Chapman is a Russian national who was arrested in June 2010, in New York City, along with nine others, on suspicion of working for a spy ring under the Russian Federation's external intelligence agency, the SVR (Sluzhba Vneshney Razvedki). She was arrested shortly after meeting with an FBI agent pretending to be a Russian official.

Chapman plead guilty to conspiracy to act as an agent of a foreign government without notifying the U.S. Attorney General and was deported back to Russia in July 2010, as part of a prisoner swap, the largest since 1986.

Her fellow Russians welcomed Chapman home, and the government awarded her a medal for her work.

Her good looks made Chapman a focus of the media spotlight. Upon return to Russia, she posed for a men's magazine and walked the runway as a model for Moscow Fashion Week. She currently hosts a TV show called "Mysteries of the World," on Russian television.

THE SPY THAT BECAME A CELEBRITY

- June 28th, 2010, she was arrested with ten other Russians on charges of conspiring to act as an unregistered agent of a foreign government
- After her arrest, hundreds of (USPER3) Facebook friends quickly dropped her
- July 8, 2010, she pled guilty and was returned to Russia for four U.S. sources
- October 2010, she received highest honors from the Kremlin for her work as an undercover Russian agent

What is “Malign Foreign Influence?”

- Combating foreign influence in an interconnected world, combined with the anonymity of the Internet
- Adversaries use tools like the Internet to spread disinformation, discord, and undermine confidence in U.S. democratic institutions and values

- Foreign influence operations will evolve as technology evolves
- Use a critical eye when reading social media, check sources whenever possible

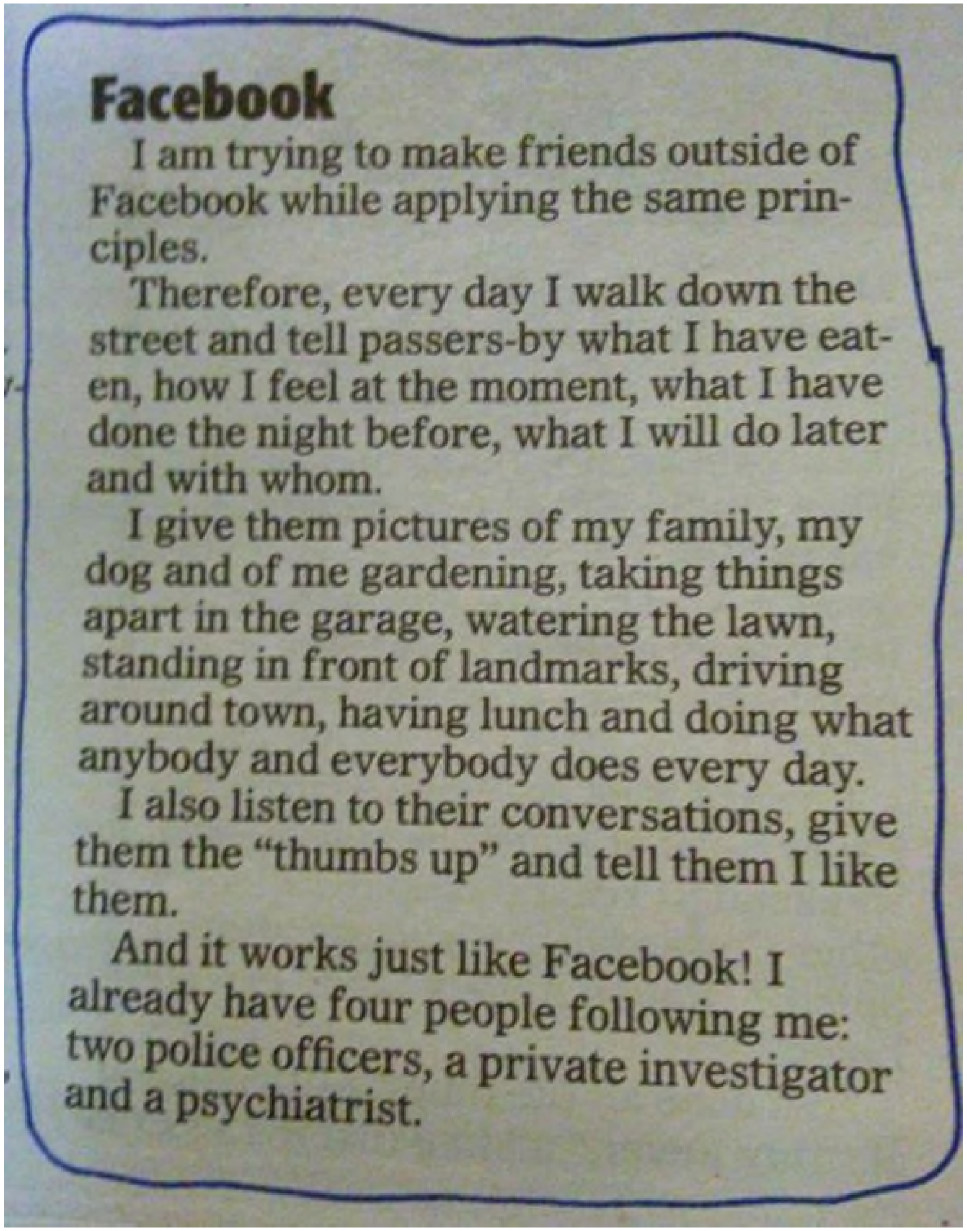
- Targeting
  - Election infrastructure (registration databases, voting machines)
  - Political organizations and Public officials
  - Public opinion to sow division

中国 @ KaitlynFondren8
Fully support the Hong Kong Police
Force to enforce laws strictly, …
riots and control chaos, m…
Hong Kong's safety –
and revive the glor…

Türkiye @akhilal_1_2
Devletinin ve milletinin hep
karşısında olan bir oluşuma
#YeteneksizsinizCHP denmez
… ne denir?

Россия @Of_Cheburash
Президент РФ Владимир Пу
выполнил гражданский долг,
проголосовав на выборах в Г
#Путин #Россия #Выборы2016

Social Media



Facebook

I am trying to make friends outside of Facebook while applying the same principles.

Therefore, every day I walk down the street and tell passers-by what I have eaten, how I feel at the moment, what I have done the night before, what I will do later and with whom.

I give them pictures of my family, my dog and of me gardening, taking things apart in the garage, watering the lawn, standing in front of landmarks, driving around town, having lunch and doing what anybody and everybody does every day.

I also listen to their conversations, give them the "thumbs up" and tell them I like them.

And it works just like Facebook! I already have four people following me: two police officers, a private investigator and a psychiatrist.

4 Things to Remember

- If you think something is an anomaly, report it (If you say no, let DCSA know!)

- Identifying & reporting vulnerabilities helps protect your product, your company, and DoD technology

- Insider Threat is the most damaging

- Do not open attachments (or click on links) from someone you do not know

Questions?

Larry Hite
200 E Palm Valley Drive
Oviedo Fl 32780
larry.f.hite.civ@mail.mil
Office: 407 542 – 6950
Mobile: 571 656 - 7897

Doug Hartwell
Tampa Fl
Douglas.e.Hartwell.civ@mail.mil
Office: 813 280 - 8861
Mobile: 813 442-2935

This brief has been produced by the Defense Counterintelligence and Security Agency (DCSA) for DoD Contractors and Government Agencies as Part of their security program. Questions and requests to further distribute this publication should be addresses to the DCSA Directorate of Counterintelligence