Naval Information Warfare Center Atlantic
Research & Technology (& Acquisition) Protection Operations Security

Charleston Defense Contractors Association
52nd Small Business and Industry Outreach Initiative
16 October 2019

Lane H. Melton Ed.D
NIWC Atlantic
Operations Security (OPSEC) Manager
Research & Technology Protection (RTP) Manager
Supply Chain Risk Management (SCRM)
Agenda

- What is RTP / OPSEC
- Government & Critical Information
- Threats to RDA
- Critical Vulnerabilities
- Risk Identification and Assessment
- Practical Countermeasures
RTP / OPSEC
Research & Technology Protection (Practical)

- RTP is an umbrella term that refers to a collection of security and security related measures taken by Programs and Projects to systematically protect Critical Technologies, their Critical Program Information (CPI) and their associated Classified, Critical and Critical Unclassified Information.
  - Made up of several elements / areas of focus
    - Assessments
      - Threats
      - Vulnerabilities
      - Risks
      - Physical
      - Technical
      - Administrative
    - Traditional Security SME (InfoSec, Physical Sec, Industrial Sec, PersSec)
    - Trusted Systems and Networks (TSN)
      - Anti-Tamper (AT)
      - Supply Chain Risk Management (SCRM)
    - Foreign Military Sales
    - Cyber Security
    - OPSEC

- RTP is an Program responsibility, vice a SECURITY responsibility
  - The IPT develops RTP measures in conjunction with supporting SMEs to protect a Program or Project
  - It is reflected / documented / disseminated in comprehensive Program Protection Plans (PPP)
Operations Security (Practical)

An **Information Protection Mindset** focused on the **Observable Indicators** that reveal Classified, Critical Program or Controlled Unclassified Information

**A Risk Analysis and Mitigation Process**
- Emphasis on Adversary **Collection Capability** and Intent
- Focused on the protection of **Essential Secrets**
  - Classified Information
  - Critical Program Information
  - Controlled Unclassified Information

**A Proactive Planning Activity**
- An **OPERATIONS** function (it is not a specialized security function)
  - OPSEC is a personal practice and the responsibility of individual program personnel
  - Integrated and part of daily operations.
  - Used to identify and Coordinate Anyth
Operations Security (Practical)

OPSEC Objectives

- Ensure that no sensitive information is disclosed that would hurt / disadvantage U.S. personnel, capabilities, operations or plans NOW or in the FUTURE
- Ensure that no sensitive information is disclosed that would provide an adversary with an advantage.
- Provide personnel and programs with information required to develop effective countermeasures.

These objectives help ensure that NIWC Atlantic:

1. Maintains critical competitive advantages for the Navy and the U.S. Military
2. Achieves its Missions
3. Protects Facilities, Employees, Partner Organizations, and Operations

Statement A: Approved for Public Release. Distribution is unlimited (15 October 2019).
Basic Broadly Applicable Concepts

5 Basic Steps

**STEP 1** Identify Critical Information …… **What are we (really) trying to protect?**
- Information we must protect to ensure our success or that an adversary needs to prevent our success.
- **Specific facts (or evidence)** about friendly intentions, capabilities, and activities needed by adversaries to plan and act effectively against friendly mission accomplishment.

**STEP 2** Analyze the Threat …… **Who are the Bad Guys?**
- **Any entity (person, government, company, organization)** that has both capability and intent to do harm to the United States or you.
- **OPSEC Indicators:** are **friendly detectable actions** and open source information that can be interpreted or pieced together by an adversary to derive critical information.

**STEP 3** Analyze Vulnerabilities …… **How are they going to get the information?**
- **Actions** that provide direct or indirect avenues to information that may be gathered and evaluated by the adversary.
- **OPSEC Vulnerability:** A **condition** in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making.

**STEP 4** Assess Risk …… **What is the Impact?**
- **Evaluation/assessment** of the vulnerabilities and threats, and the potential impact due to loss or compromise of information.

**STEP 5** Apply Countermeasures …… **How can you help stop them?**
- **Solutions** that effectively mitigate an adversary’s ability to exploit vulnerabilities and that reduce or eliminate risk.
- **OPSEC Measure:** Methods and Means to gain and maintain **Essential Secrecy**.

Statement A: Approved for Public Release. Distribution is unlimited (15 October 2019).
Critical Information
# What Are We Protecting?

## Program Protection Planning

<table>
<thead>
<tr>
<th>Technology</th>
<th>Components</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What: Leading Edge Research and Technology</strong></td>
<td><strong>What: Mission-Critical elements</strong></td>
<td><strong>What: Applications, Processes, Capabilities, Effects, Requirements, Operational Signatures, etc.</strong></td>
</tr>
<tr>
<td>Who Identifies: System Engineers; Developers</td>
<td>Who Identifies: System Engineers, Logisticians</td>
<td>Who Identifies: All</td>
</tr>
<tr>
<td>Most Significant Threat: Adversary Intelligence Collection</td>
<td>Most Significant Threat: Supply Chain compromise (malicious insertion, clones, counterfeits)</td>
<td>Most Significant Threat: Adversary Intelligence Collection</td>
</tr>
<tr>
<td>Common Countermeasures: Classification, Export Controls, Security, Foreign Disclosure limits, Anti-Tamper, OPSEC</td>
<td>Common Countermeasures: SCRM, Anti-counterfeit program, SW / HW Assurance, trusted Supplier, OPSEC</td>
<td>Common Countermeasures: Information Assurance, Classification, Disclosure / Publication controls, Security, OPSEC, etc.</td>
</tr>
<tr>
<td>Focus: “Keep the Secret Stuff IN; protect access to / knowledge of key technology”</td>
<td>Focus: “Keep the Bad Stuff OUT”; protect / verify key components</td>
<td>Focus: “Keep the Critical Information under CONTROL”, by protecting key indicators</td>
</tr>
</tbody>
</table>

---

Statement A: Approved for Public Release. Distribution is unlimited (15 October 2019).
The point of reference is Always the **Essential Secrets** of program or product (**CPI / Classified / CUI**)
- What makes the thing **Important** or what makes it **Actually Work**
- What is the **Mission**, **Purpose** or **Intent**
- What are the **Effects** that it creates

**OPSEC planning identifies the **Observable Indicators** or **Clues** that will provide a clue to what the Essential Secrets are.**
- **Physical**: Travel, Work Activity, Structures, Equipment
- **Technical**: Emissions, Communications, Network Behavior
- **Administrative**: Publications, Contracts, Diagrams, Applications, Work Requests, Evaluations, etc, etc, etc,
CRITICAL INFORMATION: Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.

……..Information an Adversary needs to Prevent our success

……..Information We must protect to Ensure our success

***If it is Important to the program or the DoD…it is important to an Adversary***
Observable Indicators

Not just the **direct** plans or details…

…The information that allows adversaries to **DEDUCE**
the plans or details!

- Applications of new techniques and technology
- Test and employment locations
- Supported organizations and operations
- Current and future capabilities…or **lack** of capability
- Conditions or tools which limit or disrupt capabilities

Fitness app Polar revealed not only where U.S. military personnel worked, but where they lived

by Rebecca Tan 18 July 2018, *The Washington Post*

Less than seven months ago, a group of journalists and Internet sleuths reported that the fitness-tracking application Strava was revealing highly sensitive information about U.S. military personnel around the world, including in Iraq and Syria. The security breach, which alarmed lawmakers and Pentagon officials, prompted the U.S. military to launch a review of its guidelines for wireless devices at military facilities.

Now, a group of reporters in the Netherlands has found another fitness app that may have placed U.S. military personnel at even greater risk.
Threats to RDA
Common Threats

Conventional Threats

- Foreign Intelligence Entities (Spies)
- Terrorists

Unconventional Threats

- Careless and talkative individuals
- Industry Partners
- Academic Partners

Third-Party Associates

- Professional Peers
- Program Sponsors
- End – Product Users

Criminals (Organized, Opportunistic)

- Cyber
- Supply Chain

---

US intelligence warns China is using Student Spies to steal secrets

By Zachary Cohen and Alex Marquardt, CNN
Updated 9:22 PM ET, Fri February 1, 2019

Beijing is leaning on expatriate Chinese scientists, businesspeople and students like Ji -- one of roughly 350,000 from China who study in the US every year -- to gain access to anything and everything at American universities and companies that’s of interest to Beijing, according to current and former US intelligence officials, lawmakers and several experts.

The sheer size of the Chinese student population at US universities presents a major challenge for law enforcement and intelligence agencies tasked with striking the necessary balance between protecting America’s open academic environment and mitigating the risk to national security.

While it remains unclear just how many of these students are on the radar of law enforcement, current and former intelligence officials told CNN that they all remain tethered to the Chinese government in some way, even if the vast majority aren't sent to the US to spy.

It's part of a persistent, aggressive Chinese effort to undermine American industries, steal American secrets and eventually diminish American influence in the world so that Beijing can advance its own agenda, US officials, analysts and experts told CNN.

---

The Unrealized Value of Open Source Intelligence for Irregular Warfare

By Riley Murray July 25, 2019

On any given day, Facebook adds 500,000 new users, which equates to 6 new profiles every second. Five million Tweets are sent every day, roughly 5,000 tweets a second. By 2014, Google had indexed over 30 trillion internet pages, a number that continues to grow dramatically as content is generated at an exponentially increasing rate.[1] While this interconnectness has allowed society to take great leaps forward, social media and the internet remain an ungoverned space for nefarious actors.

Violent extremist organizations, criminal groups, and state actors have all taken advantage of the anonymity and access afforded by modern technology to plan, execute, and support operations, gaining relative superiority over traditional security structures.[2] As adversaries become more technologically savvy, the United States and its allies must become more adept at leveraging these trends.

Open source intelligence, especially when coupled with rapidly improving big data analysis tools, which can comb through data sets that were previously too complex to derive meaningful results, has the potential to offset this growing problem, providing intelligence on enemy forces, partners, and key populations.

---

People are key to securing the defense-industrial supply chain

By George Kamis. 14 May 2019

The process starts with people. They are responsible for ensuring that the solutions that comprise the supply chain work as designed and are inherently secure. They work closely with highly sensitive and proprietary information that is attractive to enterprising hackers. They are the first line of defense.

Unfortunately, those same factors make people the most attractive attack vector. When a malicious actor wants to gain access to a component or system, it’s often easier to just steal someone’s credentials than it is to try and find their way around a firewall. Obtaining a simple password is often enough to gain access to a critical system that can then be compromised, or information that can be exploited.

Consider the well-publicized Sea Dragon hack. In that incident, Chinese hackers obtained sensor data, signals data, an electronic warfare library and more. The hackers targeted a contractor of the Naval Undersea Warfare Center, a research and development organization that is part of the Defense Industrial Supply Chain. They used that person’s credentials to access the treasure trove of data on the NUWC network, and the supply chain was compromised.
Threats are a combination of foreign intelligence, terrorist organizations, and others all seeking these targets:

- **SME’s!!** “Facilities developing, applying, or modifying highly sought after technologies are at a higher risk from foreign collectors.”
  
  - **Aeronautic Systems**
  
  - **C4I Systems**
    - Antenna, Digital Receivers, Microwave Filters, Cloud Computing, Airborne & Tactical Radios, SIGINT Systems
  
  - **Electronics**
    - Radiation-hardened or Monolithic Integrated Circuits (ICs), Gallium Nitride Amplifiers, RF Attenuators
  
  - **Optics**
    - Fast Steering Mirrors, Night Vision Devices, Infrared Interference Filters, Thermal Imaging Cameras, Wide Area Optical Systems
  
  - **Marine Systems**
    - Autonomous Underwater and Surface Vehicles, Underwater Detection Technologies
  
  - **Software**
    - Modeling and Simulation, Facial Recognition, Computer-aided Design (CAD), Wide Area Surveillance
Critical Vulnerabilities
Conduits of Information

Our means of communication / collaboration are their means of intelligence collection

- Be cognizant of work occurring at less secure third-party facilities vendors / partner labs / end user sites
- Temporary work locations (travel, telework)
- You must consider where the information will go BEYOND who you give it to directly (Who will they give it / provide access to?)
- Common Issues
  - Conversations in Public Areas
  - Using unsecure communications means (cell)
  - Web page posting (Official & Social Media)
  - Professional Publication (journals, patents, awards)
  - Industry Publication (contracts, advertisements)
  - Organizational Association (Badge & CAC display / open access areas / government assets)
  - Unauthorized Photography
Data Aggregation is what they are after

Information collection from multiple sources which can be pieced together to:

- Develop an accurate and comprehensive profile of you (who, what, when, where, how)
- Provide them with enough information to allow complete access to your most sensitive data
  - **Funding** (source / supported users, mission, associated programs)
  - **Operations** (locations, frequencies, timing)
  - **Personnel Information** (individual targets / potential access, work sites, travel / employment trace)
  - **Procurement** (project characteristics, status, associated COTS / system vulnerabilities)

*Manchester Document*: an Al Qaeda recruit training handbook which specified that open and public sources accounted for 80% of all information collected
Practical Countermeasures
Countermeasures

Countermeasures are **LEAST Effective After the Fact**, i.e., if they are added on to or applied to program after decision are made or actions taken ....they should be considered as part of the event / operation / development / creation From The Start (“Baked In” to any publications, CRADA, contracts, PPP, T&E, transport, installation, component procurement, training, etc…).

- Countermeasures are **Anything** that effectively **Negates** or **Reduces** an adversary’s ability to compromise or exploit us

- **What can you do to stop them?**
  - **Follow the published guidance**
    - Do not circumvent Network or Facility Policies
    - Use Protected Communications (ensure all your communications are protected in some way)
  - Make the security of the information an **Key Initial Requirement for ANY action.**
  - **Do Not Disregard Security** in preference for expediency
    - Be Alert
    - Be Suspicious
    - Be Proactively Paranoid
    - Watch what you are saying, regardless of the audience or location

Statement A: Approved for Public Release. Distribution is unlimited (15 October 2019).
Conclusion
The Impact of Unclassified Information

▼ The processes (Critical Info, Threat, Vulnerability, Risk, Countermeasures) are designed to be applied **At The Beginning** of a project.

- From the very **inception** of an idea / proposal
- To avoid ineffective compensatory measures after the information has been released to the wider public

▼ Why protect unclassified information? Because unclassified information can be important, and – like classified information – of significant value to an adversary. (The September 11, 2001 terrorist attacks were planned and executed **without** classified information.

▼ The OPSEC process is essential to protecting Controlled Unclassified **AND** Classified information and helps personnel more accurately understand the risks of their decisions.

- OPSEC and RTP requirments cover **ALL** SPAWAR and supported activities t
- Critical Information/CPI are intrinsic to any military RDTE/Acquisition activities and missions
- Sharing information is intrinsic to the activities and mission and must be accounted for
Serve our Nation by delivering information warfare solutions that protect national security.

WIN THE INFORMATION WAR.

NIWC Atlantic is part of the Naval Research & Development Establishment (NR&DE)

Glassdoor: https://www.glassdoor.com/Overview/Working-at-SPAWAR-Systems-Center-Atlantic-EI_IE638508.11,41.htm
NAVWAR Contract Directorate Office: https://e-commerce.sscomo.nmci.navy.mil

Statement A: Approved for Public Release. Distribution is unlimited (15 October 2019).