The Need: Thwarting the adversary by analyzing Cyber behaviors



Why Cyber is Integral?

President's Comprehensive National Cybersecurity Initiative

 Develop and implement a government-wide cyber counterintelligence (CI) plan

ONCIX CI Strategy: Detect and Counter FISS Cyber

- Unifying Intelligence Strategy for Cyber, 11 Mar 2013
 - Cyber Intelligence must be presented in a holistic fashion (threat, vulnerability and value)
 - All-Source

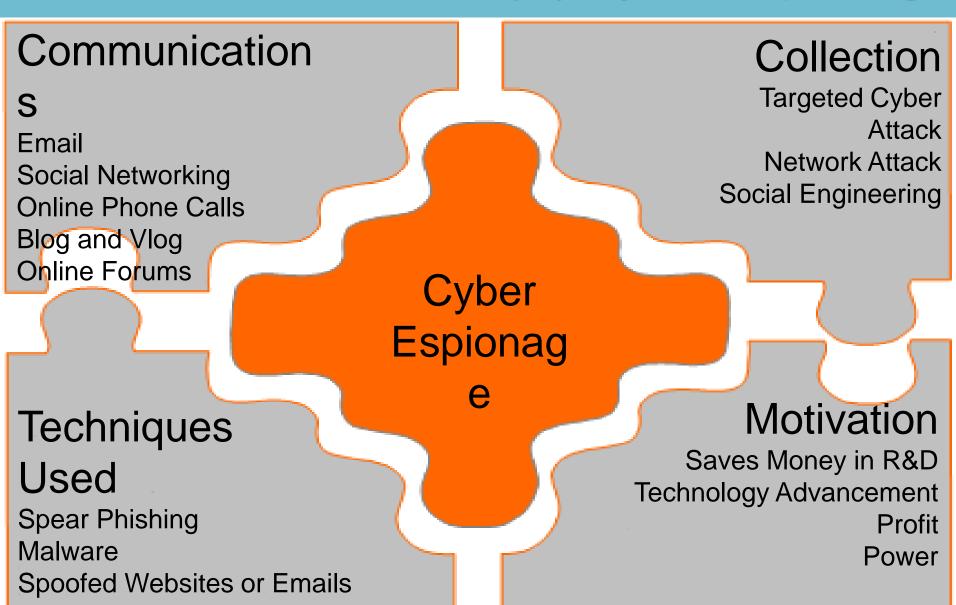
Defense Science Board

- Defense only is a failed strategy
- Threat, Vulnerability and Consequence cannot be managed in isolation
 - ThindatOstapopteen into two categories: adversaries in the standed the stander pabilities

"In this [Cyber] threat environment, the importance and urgency of intelligence integration cannot be overstated."

"The theft of intellectual property is the biggest transfer of wealth in history, from this nation to others."

(U) Cyber Espionage



Anatomy of the Acquisition Cycle

Planning

Plan on how to act on their motivation and intent.

Targeting

Target victims, whether by sector, or technology hardware or software, or some combination of factors.

- HUMINT
- Cyber
- Blended
- Financial
- Supply Chain

Design tactics, techniques, and procedures they will employ during their attack.

- Cleared
 Contractor
- Sub Contractor
- Research
 Lab
- Academia

Design

- Spear Phishing
- Malware
- Spoofed Websites or Emails

Logistics

Logistics for acquiring funding for time and resources, leveraged infrastructures, and other supporting elements such as people or technology needed for the attack.

- Knowledge
- Manpower
- TIME

Weaponization

Weaponization is the act of developing a set of weapons

Exercise

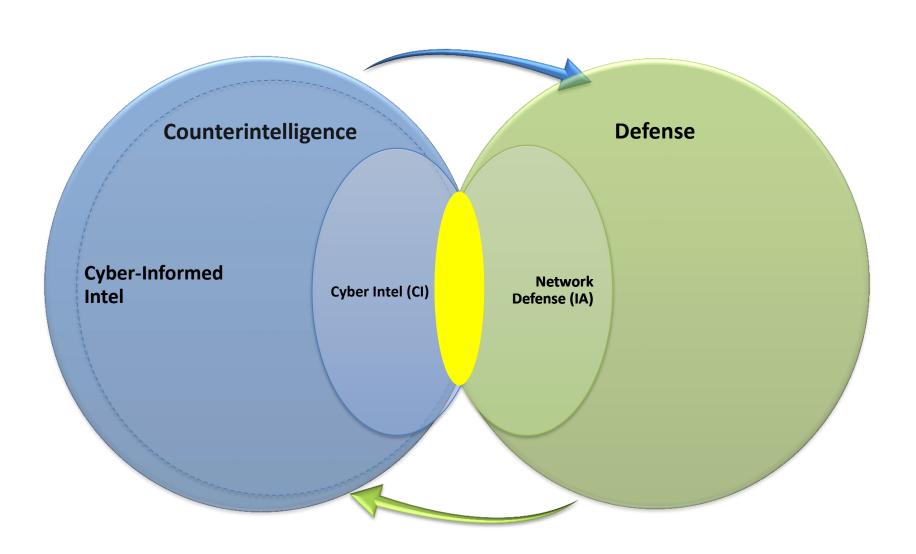
Exercise to test and practice to ensure it actually works with at least some degree of certainty.

- Exploit the vulnerability
- Network
- Extranet
- VPN
- Human

- Sandbox
- Third Party/ private user

40% 30% 20%

Mutually Supportive Missions



UNCLASSIFIED

(U) Using Cyber to our Advantage

• (U) Landscape:

- (U) Network defense is one part of the strategy
- (U) Threats begin and end with a human
- (U) Cyber intelligence must be presented in a holistic fashion (threat, vulnerability and value)
- (U) 70% of all counterintelligence case referrals by DSS involve cyber activity

(U) Anticipatory Analysis:

- (U) Left of the cyber "boom;" get ahead of the threat
- (U) The infectious spread? The "spider web" in cyberspace interconnected
- (U) Indicators begin with: cyber incident and/or consequence/value
- (U) Many Sensors/Many data elements

Questions?

When you change the way you look at things, the things you look at change.



– Max Planck (Nobel Physicist)

Questions