SPAWAR

Systems Center
ATLANTIC

'FOR OFFICIAL USE ONLY'

Space and Naval Warfare Systems Center Atlantic

An Overview of the Cyber Warfare, Exploitation & Information Dominance (CWEID) Lab

Presented to the CDCA Small Business & Industry Outreach Initiative Symposium

Vincent Van Houten, GSLC
IA Engineering & Cyber Defense Division, 58200

Date: 28 January 2010

Opening Statements

'FOR OFFICIAL USE ONLY'

- Never before has it been possible for one person to potentially affect an entire Nation's security.
- In 1999 (10 years ago), two Chinese Colonels published a book called "Unrestricted Warfare" that advocated "not fighting" the U.S. directly, but "understanding and employing the principle of asymmetry correctly to allow us [the Chinese] always to find and exploit an enemy's soft spots."
- The idea that a less-capable foe can take on a militarily superior opponent also aligns with the views of the ancient Chinese general, Sun Tzu. In his book "The Art of War," the strategist advocates stealth, deception and indirect attack to overcome a stronger opponent in battle.

Cyberspace is a Domain - The Principles of War Apply

Cyber Defined

According to the S.773 Bill (Cybersecurity Act of 2009) the term ‘Cyber’ means:

- any process, program, or protocol relating to the use of the Internet or an intranet, automatic data processing or transmission, or telecommunication via the Internet or an intranet; and
- any matter relating to, or involving the use of, computers or computer networks.

Cyber Crosses All Domains – Sea – Air - Land - Space

Cyber Warfare

- In lieu of a Concise Definition
  - **Cyber Warfare**, warfare conducted in Cyberspace, is essentially any act intended to compel an opponent to fulfill our national will, executed against the software, hardware, and firmware controlling processes within an adversary's system.
- Electronic Warfare
  - An Overlapping Discipline (e.g. 802.11 Wireless, EMP)
  - Actions involving the use of the electromagnetic spectrum or directed energy to control the spectrum
- Information Operations (IO) / Computer Network Operations (CNO)
  - Computer Network Attack – Exploitation – Defense (CNA/CNE/CND)

Full Spectrum Offensive & Defensive Capabilities

The Nucleus of Cyber Warfare Strategy

- Core elements required to create a highly effective Cyber Warfare Strategy:
  - **Intelligence Fusion and Collaboration**
    - Combine intelligence from multiple sources in order to achieve inferences.
  - **Cyber Surveillance and Target Acquisition**
    - Ability to detect system compromise and assist in determining who was behind the attack.
  - **Adaptive Cyber Attack Countermeasures**
    - Capability to counterattack an incoming threat thereby destroying/altering its ability in such a way that the intended effect on the target is significantly impeded.

Keys to an Effective Cyber Warfare Strategy

Requirements Traceability

‘FOR OFFICIAL USE ONLY’

- The President’s Comprehensive National Cybersecurity Initiative (CNCI)
  - Establish a front line of defense
  - Demonstrate resolve to secure U.S. Cyberspace & set conditions for long-term success
  - Shape the future environment to demonstrate resolve to secure U.S. technological advantage and address new attack and defend vectors

Customer Requirements Drive Our Response

CNCI Interdependent Portfolio to Address Cyber Security Challenges

Focus Area 1

- Trusted Internet Connections
- Deploy Passive Sensors Across Federal Systems
- Pursue Deployment of Intrusion Prevention System

  (Dynamic Defense)
- Coordinate and Redirect R&D Efforts

Establish a front line of defense

Focus Area 2

- Connect Current Centers to Enhance Cyber Situational Awareness
- Develop a Government Wide Cyber Counterintelligence Plan
- Increase the Security of the Classified Networks
- Expand Education

Demonstrate resolve to secure U.S. cyberspace & set conditions for long-term success

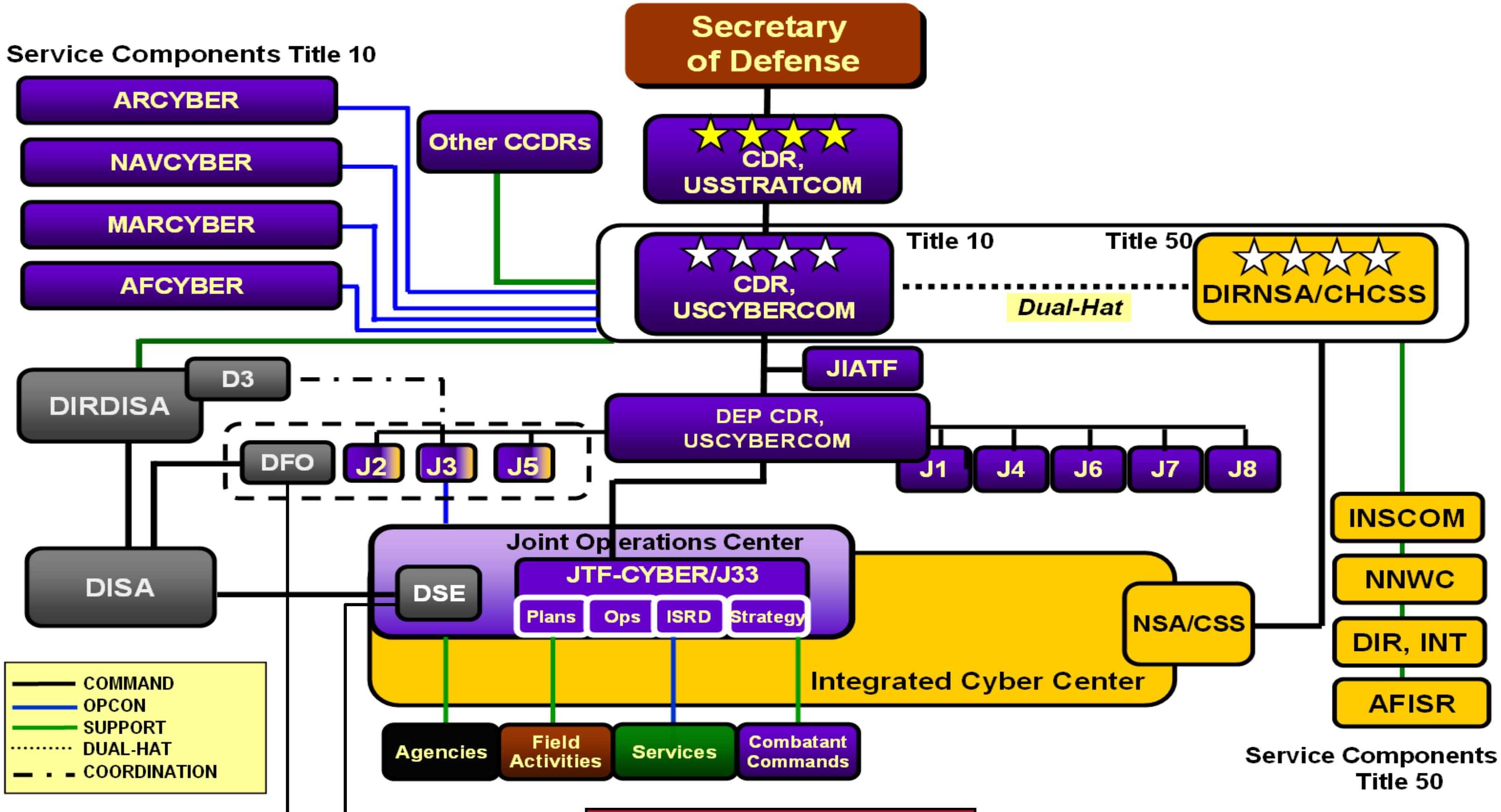
Focus Area 3

- Define and Develop Enduring Leap Ahead Technology, Strategies & Programs
- Define and Develop Enduring Deterrence Strategies & Programs
- Develop Multi-Pronged Approach for Global Supply Chain Risk Management
- Define the Federal Role for Extending Cybersecurity into Critical Infrastructure Domains

Shape the future environment to demonstrate resolve to secure U.S. technological advantage and address new attack and defend vectors

Today's Cyber Security Challenges

USCYBERCOM Organization



DISA Field Office (DFO)

- Director's liaison to USCYBERCOM
- Forward-based at Fort Meade
- Target: 50% manning NLT 1 Oct 2009

DISA Support Element (DSE)

- Liaison between Joint Operations Center (JOC) and DISA Operations
- Shared Situational Awareness
- Embedded in JOC (24 x 7)

FOUO

Requirements Rally A Solution

‘FOR OFFICIAL USE ONLY’

- The Cyber Warfare, Exploitation & Information Dominance (CWEID) Lab – **“Seaweed”**
  - A laboratory environment that models & simulates Computer Network Attacks, Exploits, and Defenses.
    - Commissioned in January of 2009 with the **Structured Holistic Attack Research Computer Network** (SHARCNet 1.0) Innovation Award
    - A Structured Net-Centric Battlespace or Cyber Range was created with $100K of government labor and $500K of reclaimed & donated GFE/GFM (HW/SW Components).
  - Fully Demonstrated and Located in Building 3113 - SSC-LANT Charleston.
  - Described as a Pioneering Approach to the Future of Cyber Warfare.

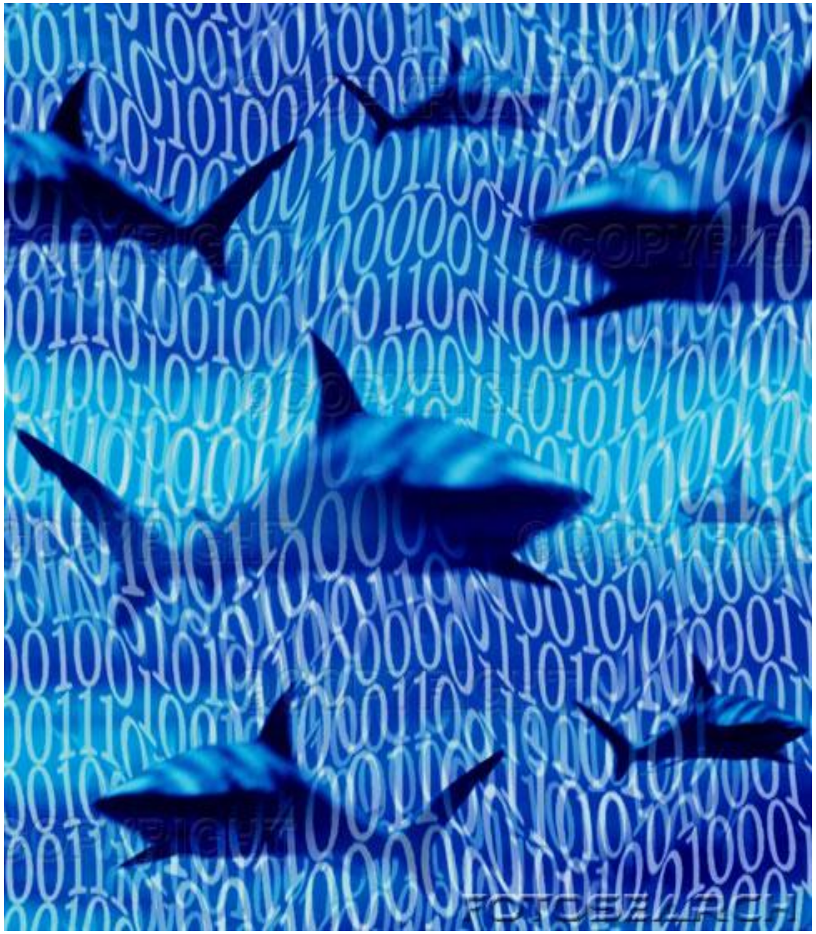
Innovations Create Advanced Solutions

The Structured Holistic Attack Research Computer Network (SHARCNet)

‘FOR OFFICIAL USE ONLY’

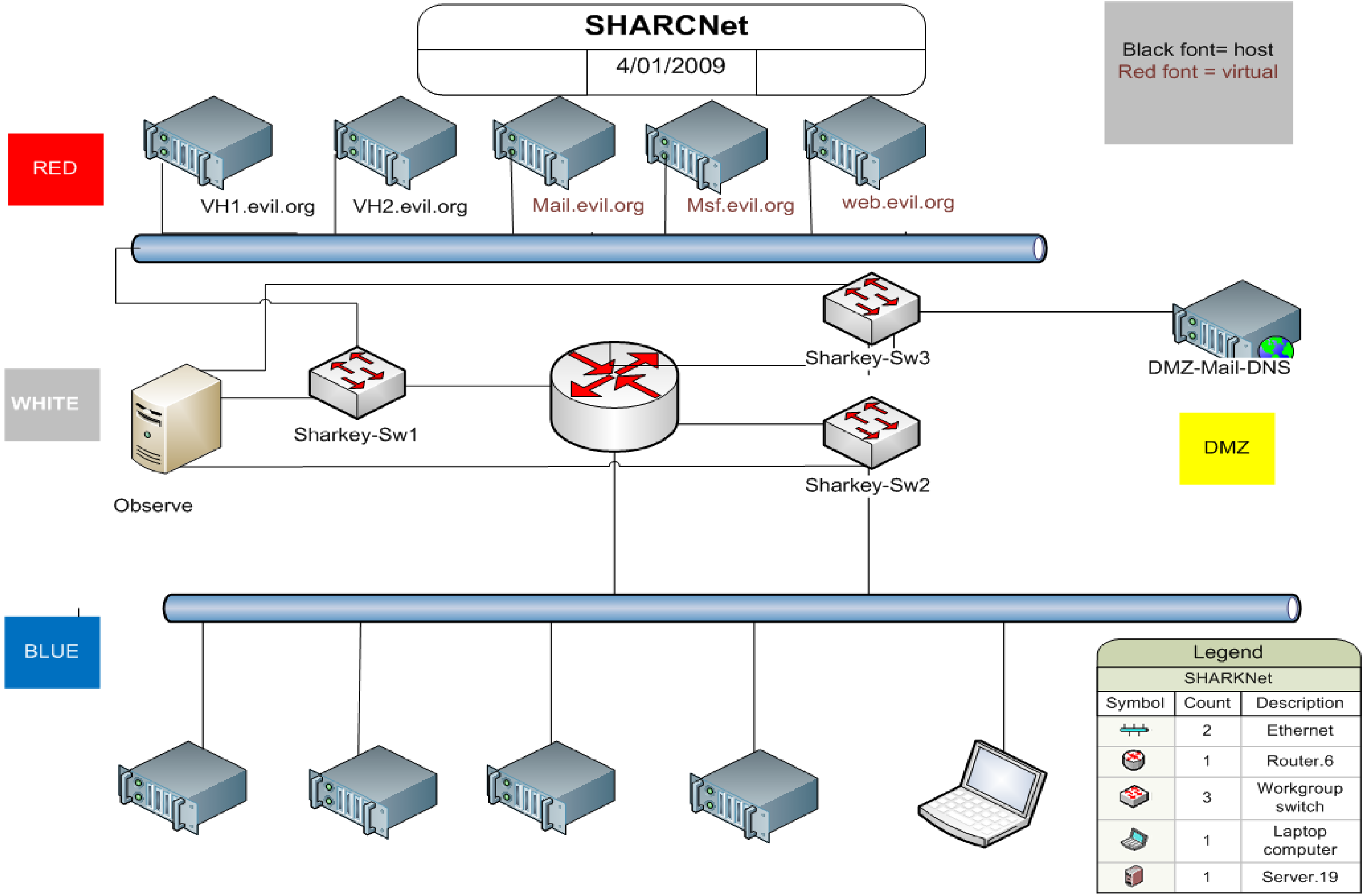
Overview

- SHARCNet allows for the Research, Development, Testing, and Evaluation of the most state of the art technologies for Cyber Warfare & Security.
- Structure
  - Red Cell fully demonstrates CNA/CNE vectors
  - Blue Cell fully demonstrates CND Defense-in-Depth Strategies and contains:
    - An Armored or Hardened Segment (Citadel)
    - A Vulnerable Segment (Victim)
  - White Cell provides Qualitative and Quantitative Cyber Security Analysis, Digital Forensics, & Autopsy.



Cyber Warfare Modeling & Simulation

Cyber Range System Architecture



SHARCNet

4/01/2009

Black font= host
Red font = virtual

Legend

SHARKNet

Symbol	Count	Description
═	2	Ethernet
⊗	1	Router.6
▣	3	Workgroup switch
💻	1	Laptop computer
▮	1	Server.19

Computer Network Attack (CNA)

‘FOR OFFICIAL USE ONLY’

▼ SHARCNet RED Cell Operations

- Includes actions taken via computer networks to disrupt, deny, degrade, or destroy the information within computers and computer networks and/or the computers/networks themselves.
- The Four D’s of CNA
  - **Degrade**
    - Data Corruption
  - **Disrupt**
    - Malicious Code, Weapons of Mass Disruption (WMD)
  - **Deny**
    - Distributed Denial of Service (DDOS), BotNets
  - **Destroy**
    - Permanent Denial of Service (PDOS), Non-Kinetic / Kinetic Response

Network Attack Modeling

Computer Network Exploitation (CNE)

‘FOR OFFICIAL USE ONLY’

- Enhanced RED Cell Operations
  - Includes enabling actions and intelligence collection via computer networks that exploit data gathered from target or enemy information systems or networks.
    - Cyber Intelligence Compilation
    - Cyber Surveillance
    - Cyber Reconnaissance
    - Cyber Counterintelligence

Network Exploitation Modeling

Computer Network Defense (CND)

‘FOR OFFICIAL USE ONLY’

▼ SHARCNet BLUE Cell Operations

- Includes actions taken via computer networks to protect, monitor, analyze, detect and respond to network attacks, intrusions, disruptions or other unauthorized actions that would compromise or cripple defense information systems and networks.
- The Defense-in-Depth approach is to defend a system against any particular attack using several, varying methods. It is a layering tactic which was conceived as a comprehensive approach to information and electronic security.
- Substructure includes:
  - A Citadel Segment (Armored – Dynamic Defense)
  - A Victim Segment (Vulnerable)

Network Defense-in-Depth Modeling

CNO Monitoring & Collection

‘FOR OFFICIAL USE ONLY’

- SHARCNet WHITE Cell Operations
  - Neutral Objectives
    - Observe
    - Monitor
    - Collect
    - Analyze (Digital Forensics & Autopsy)
    - HoneyNet / HoneyPot Analysis

Real-time Research & Analysis

Scenario 1 Overview

- **Goal: Obtain very specific information (financial, contract information, passwords, sensitive employee data, classified info, etc.)**
- **Motivation: Cyber Espionage**
- **Vector: Spear Phishing Attack**
- **Target: Project “Tiburón Dulce” a.k.a USS Aumakua**
- **Details:**
  - Attacker finds that there is an open “ALL HANDS” e-mail list or employee contact page on the Internet by searching Google for +“employee contacts” +site:mil.
  - Attacker settles on a command at rawaps.navy.mil because not only do they list employee names and email addresses they also list the person's title.
  - The attacker now spoofs an email from the Commanding Officer to his subordinates.
  - The email also directs recipients to execute a file in order to scan their systems for “security patches” and antivirus updates (actually been done…).
  - The hyperlinks are a surreptitious redirect that connects to the attacker’s website where malicious code is downloaded to exploit a well known vulnerability.
  - After gaining control of a system inside the command’s network, the attacker can now search for information and download files on his/her target - Project “Tiburón Dulce”.

Spoofed HTML-based E-mail

-----Original Message-----
From: **Shipshape, Grin CAPT RAWAPS LANTIS**
Sent: **Wednesday, April 01, 2009 8:01 AM**
Subject: **All Hands - Mandatory Security Scan on ALL Systems**
Importance: **High**

All,

The action below is MANDATORY to ensure continued network integrity and security.

This email is being sent to All Hands Atlantis (Government and Contractor).

****

This is an action email to all users of the RAWAPS RDT&E network. You MUST perform a Mandatory Security Scan of all of your systems (domain and non-domain) no later than COB Friday, May 29, 2009.

If you are on the domain, please download the file from https://rdte.chs.rawaps.navy.mil/netsec then reboot your computer and the security scan will execute automatically. Once the scan is complete, the report will automatically be sent back to the host server.

If you are not on the domain, please download the file from https://www.rawaps.navy.mil/netsec/downloads/scanner.exe and run the executable manually. Once the scan is complete, send the report.txt output file to your Command IAM or delegate immediately.

For updates regarding this scanning utility, including tools for use on Mac, Linux, and Solaris, please visit the network security website at: https://rdte.chs.rawaps.navy.mil/netsec

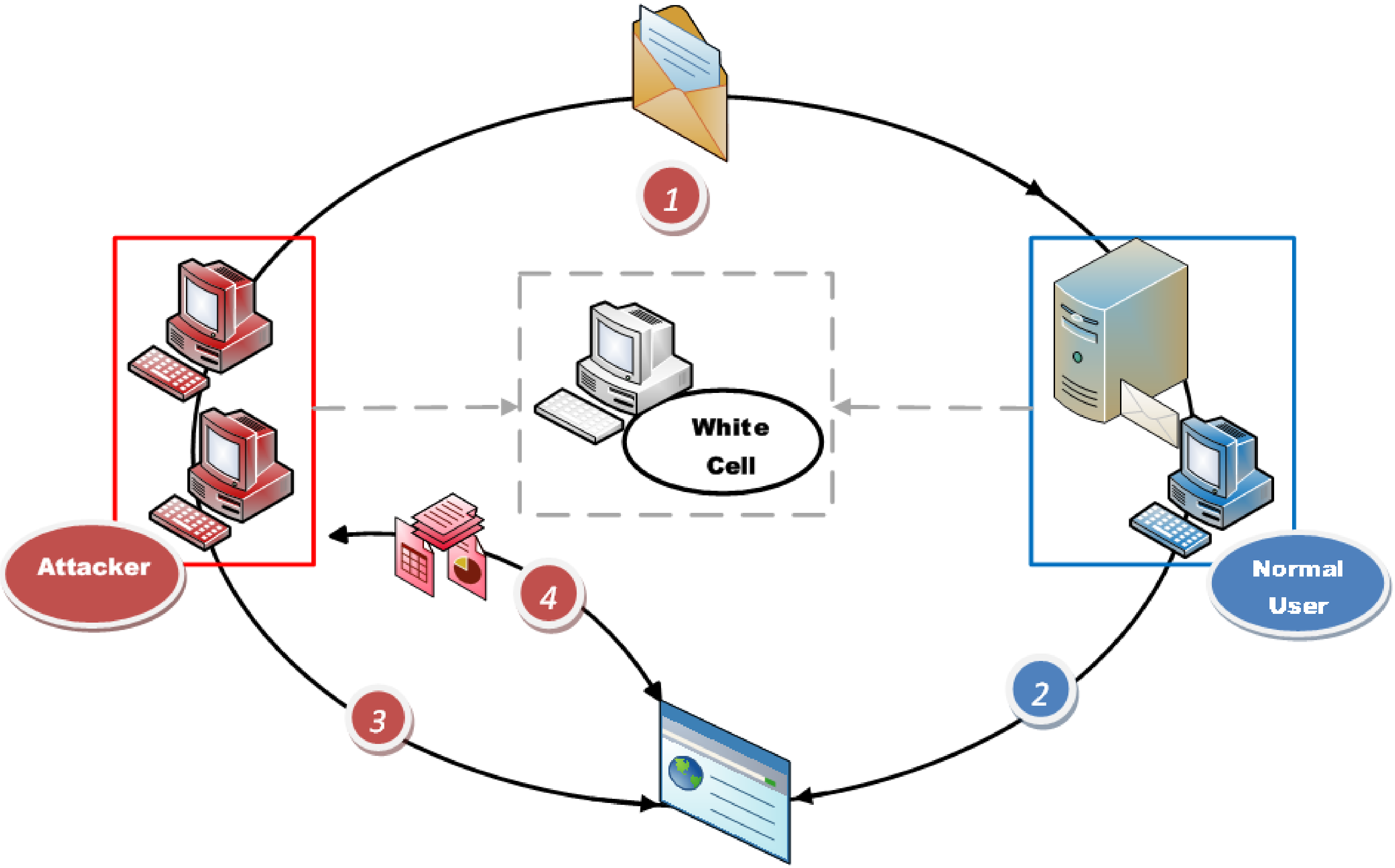
You must have a Rawaps account and CAC card to view this page.

Repeat, this is a MANDATORY Security scan. Non compliant systems will be disconnected from the network.

Sincerely,

CAPT Grin Shipshape
Commanding Officer
RAWAPSSYSCEN Atlantis
(843) 555-1212
(c) (757) 555-1212

Scenario 1 Overview



Cyber Warfare & Human Capital

‘FOR OFFICIAL USE ONLY’

The “Who” part of the Equation

- Human capital refers to the collective value of this organization's intellectual capital (competencies, knowledge, and skills); our source of creativity and innovativeness.
- Our #1 commodity walks out the door every night.

The Right Stuff

- The skill sets needed to penetrate a network for intelligence gathering purposes in peacetime are the same skills necessary to penetrate that network for offensive action during wartime.

SPAWARLANT Cyber “Top Guns”

- a.k.a. Ethical Hackers (e.g. GPEN, CEH)
- Experts with Exploit Tools (e.g. Core Impact, Metasploit)

The Human Mind is Our Fundamental Resource

CWEID / SHARCNet 2.0

‘FOR OFFICIAL USE ONLY’

▼ Setting the Next Waypoint

- **Unified Threat Management System (UTMS) RDT&E**
  - Dynamic Defense
- **Network Exploitation Test Tool (NETT)**
  - Cyber Threat Modeling
- **Mission Environment for Network Attack Computer Exploitation and Defense (MENACED)**
  - Cyber Range Management Services
- **Cyber Range in a Box (CRIAB)**
  - Low Cost, Extensible Range Environment
- **Cyber Munitions Deployment System (CMDS)**
  - Development, provisioning, deployment and execution of tactics/weapons.
- **Cyber Weapons Development**
  - Weapon Development API & Test Framework
  - Fixed & Mobile Cyber Engagement Centers

Advancing Cyber Warfare Capabilities to the Warfighter

In Summary

- A great deal of our combat capability operates in Cyberspace: Command, Control, Communications, and Computer (C4) systems as well as the Intelligence, Surveillance, and Reconnaissance (ISR) platforms.
- The cyber realm embodies far more than just network or information warfare. Cyberspace is a domain, much like sea, air, and land, where each of the principles of war applies.
- We cannot allow our adversaries to gain an advantage in Cyberspace and to operate there freely.
- We are a Systems Warfare Center and We are not here to simply maintain the status quo;

We are here to PREVAIL

Information Dominance IS Cyberspace Superiority

Questions

POC: **Vince Van Houten, GSLC**

IA Engineering & Cyber Defense Division, 58200
SPAWARLANT Charleston SC

O: 843.218.7108
D: 588.7108
F: 843.218.5461
E: vincent.vanhouten@navy.mil
URL: https://infosec.navy.mil

Backup Slides

- Moonlight Maze (1999)
  - Traced to a main frame computer in Moscow. It was claimed that these hackers had obtained large stores of data that might include classified naval codes and information on missile guidance systems.
- Titan Rain (2003)
  - These attacks were labeled as Chinese in origin, although their precise nature (i.e., state-sponsored espionage, corporate espionage, or random hacker attacks) and their real identities remain unknown.

Our Potential Adversaries are Actively Targeting the U.S.

Backup Slides

‘FOR OFFICIAL USE ONLY’

MyDoom Worm (2004 & 2009)

- Beginning on July 4, 2009 multiple U.S. Government Agencies and select private-sector companies have been victims of a what US-CERT categorizes as a massive, ongoing Distributed Denial of Service (DDoS) attack.
- The attacks were originating from one or more Botnets, consisting of compromised systems from across the globe.
- At least 9,000 IPs were identified as attack sources – some estimates put the total number of systems attacking at between 30,000 and 60,000.
- Bot self-destruct sequence initiated after the attack was countered erasing host OS.
- Attacker(s) and motivation are unknown.

Our Potential Adversaries are Actively Targeting the U.S.

NATIONAL
SECURITY
ARCHIVE

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu