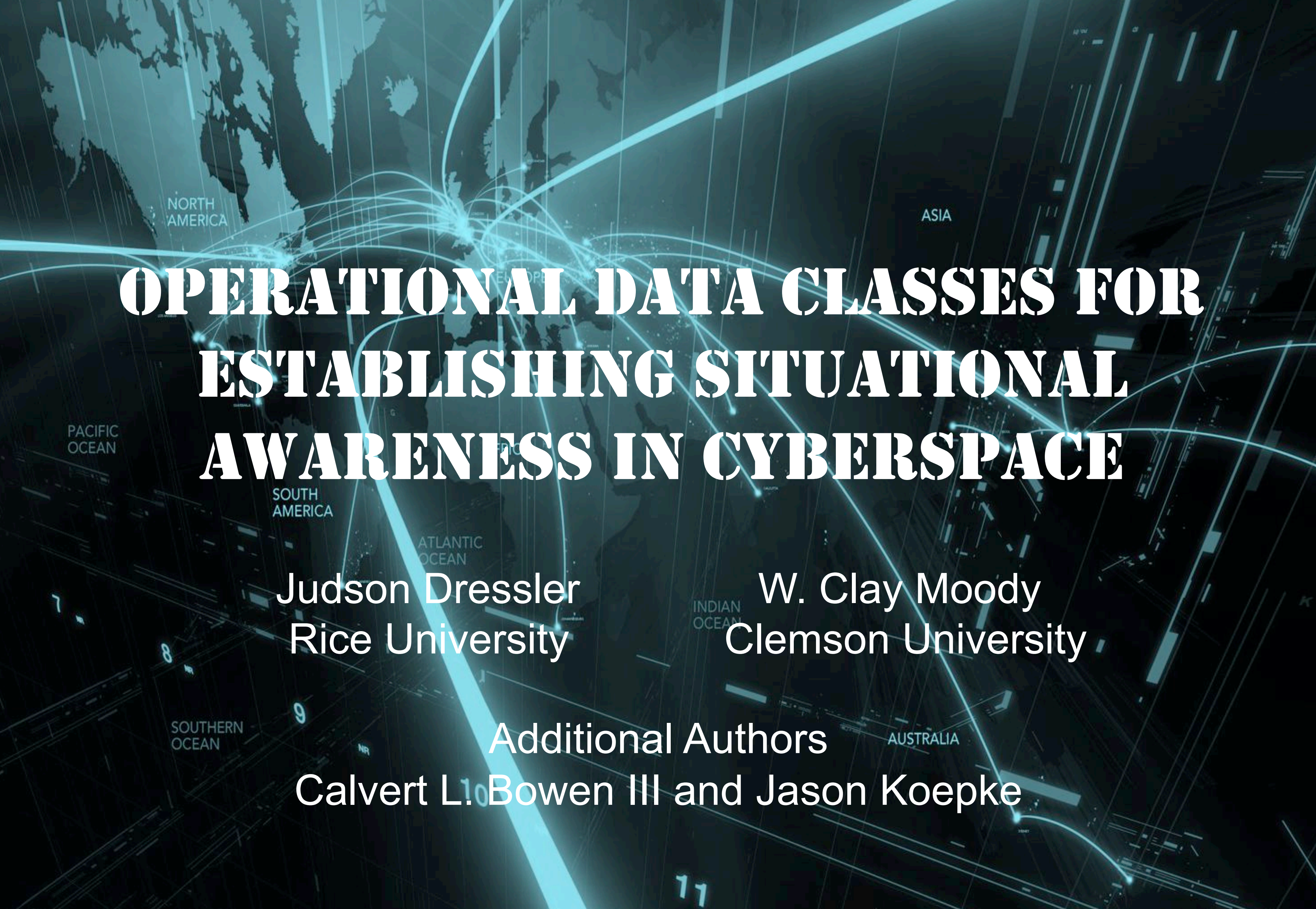


OPERATIONAL DATA CLASSES FOR ESTABLISHING SITUATIONAL AWARENESS IN CYBERSPACE

Judson Dressler
Rice University

W. Clay Moody
Clemson University

Additional Authors
Calvert L. Bowen III and Jason Koepke

Disclaimer

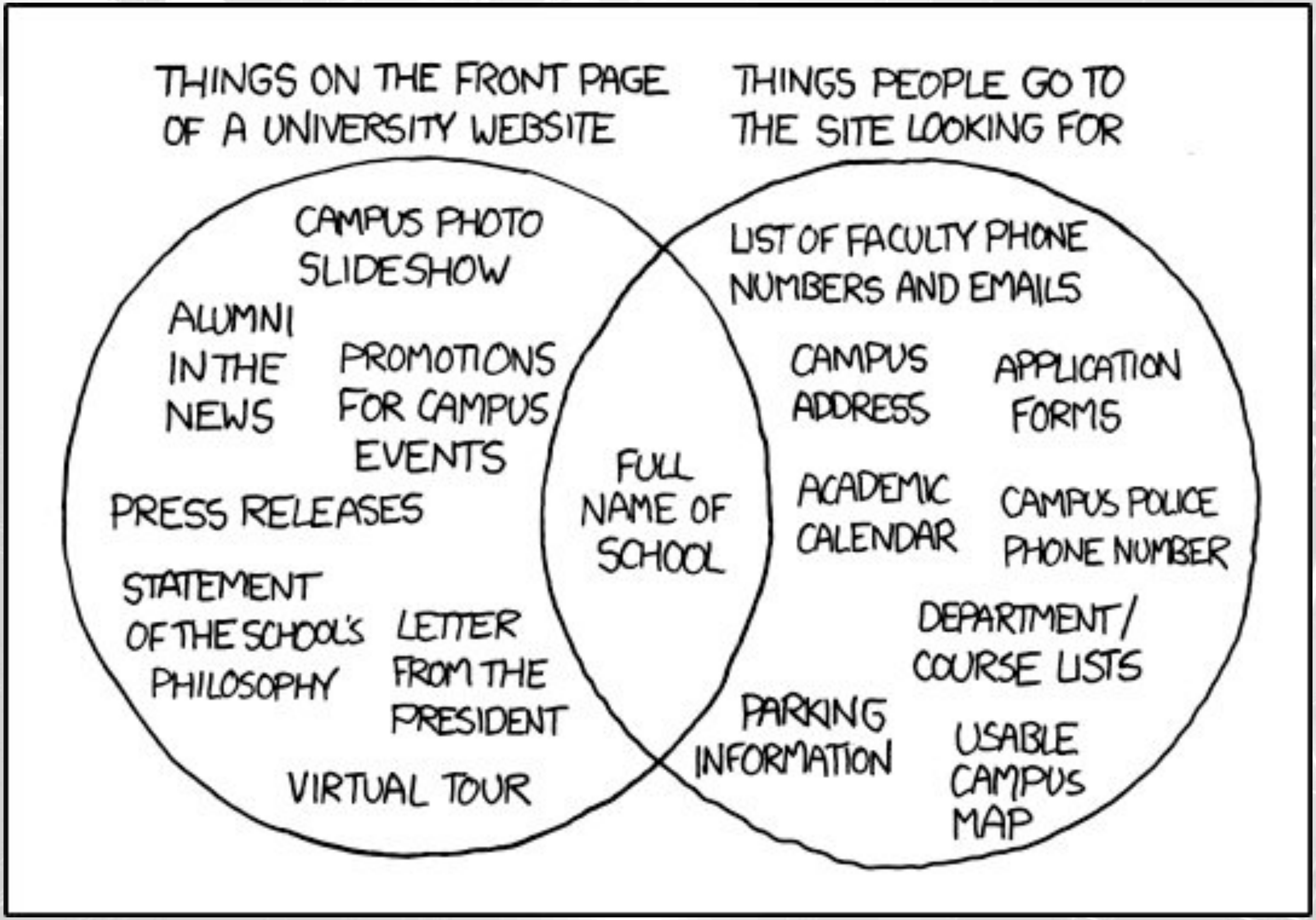
- The views and opinions expressed in this presentation are those of the authors and do not necessarily reflect those of Rice or Clemson University or the US Department of Defense

- Parts of this presentation have undergone a pre-publication review by various offices of the United States Government

Agenda

- Introduction
- Motivation
- Background Information
- Framework Overview
- Theoretical Case Study
- Challenges
- Conclusions

Cyber SA Reality?

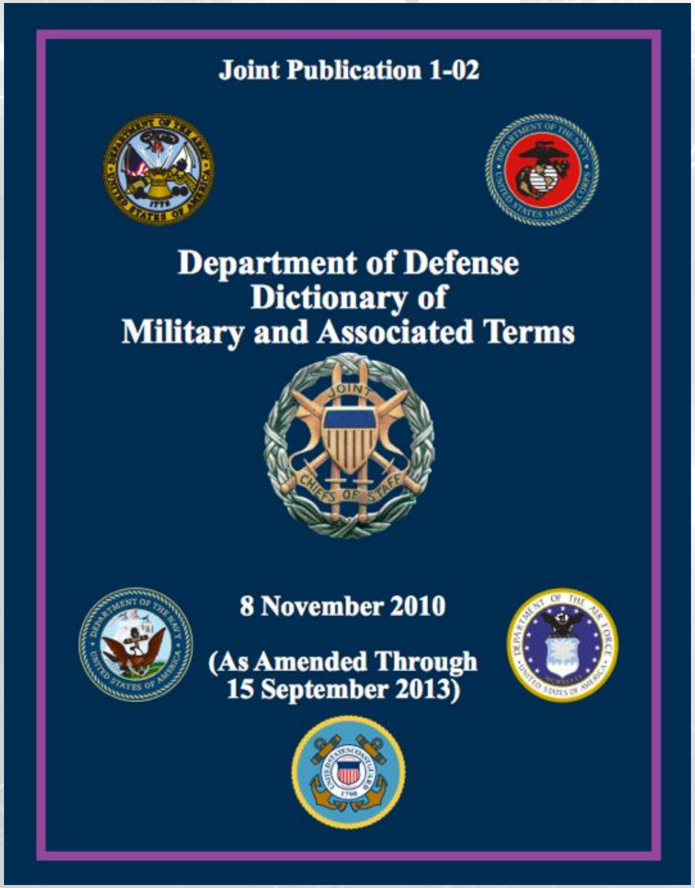

THINGS ON THE FRONT PAGE OF A UNIVERSITY WEBSITE
THINGS PEOPLE GO TO THE SITE LOOKING FOR
CAMPUS PHOTO SLIDESHOW
ALUMNI IN THE NEWS
PROMOTIONS FOR CAMPUS EVENTS
PRESS RELEASES
STATEMENT OF THE SCHOOL'S PHILOSOPHY
LETTER FROM THE PRESIDENT
VIRTUAL TOUR
FULL NAME OF SCHOOL
LIST OF FACULTY PHONE NUMBERS AND EMAILS
CAMPUS ADDRESS
APPLICATION FORMS
ACADEMIC CALENDAR
CAMPUS POLICE PHONE NUMBER
DEPARTMENT/ COURSE LISTS
PARKING INFORMATION
USABLE CAMPUS MAP

Courtesy of xkcd.com

Introduction

- National critical infrastructure has key role in:
  - Energy
  - Transportation
  - Finance
  - Defense
- Disruption of US DoD systems significantly damages ability to defend the nation
- Must understand the cyber operating environment to secure the nation

Cyberspace doctrine



Joint Publication 1-02

Department of Defense
Dictionary of
Military and Associated Terms

8 November 2010

(As Amended Through
15 September 2013)

- Cyberspace is the newest war fighting domain (with land, sea, air, and space)

- No doctrinal definition of "situational awareness" for DoD

- Closest was "battlespace awareness" but it was removed in 2011

"Knowledge and understanding of the operational area's environment, factors, and conditions, to include the status of friendly and adversary forces, neutrals and noncombatants, weather and terrain, that enables timely, relevant, comprehensive, and accurate assessments, in order to successfully apply combat power, protect the force, and/or complete the mission"

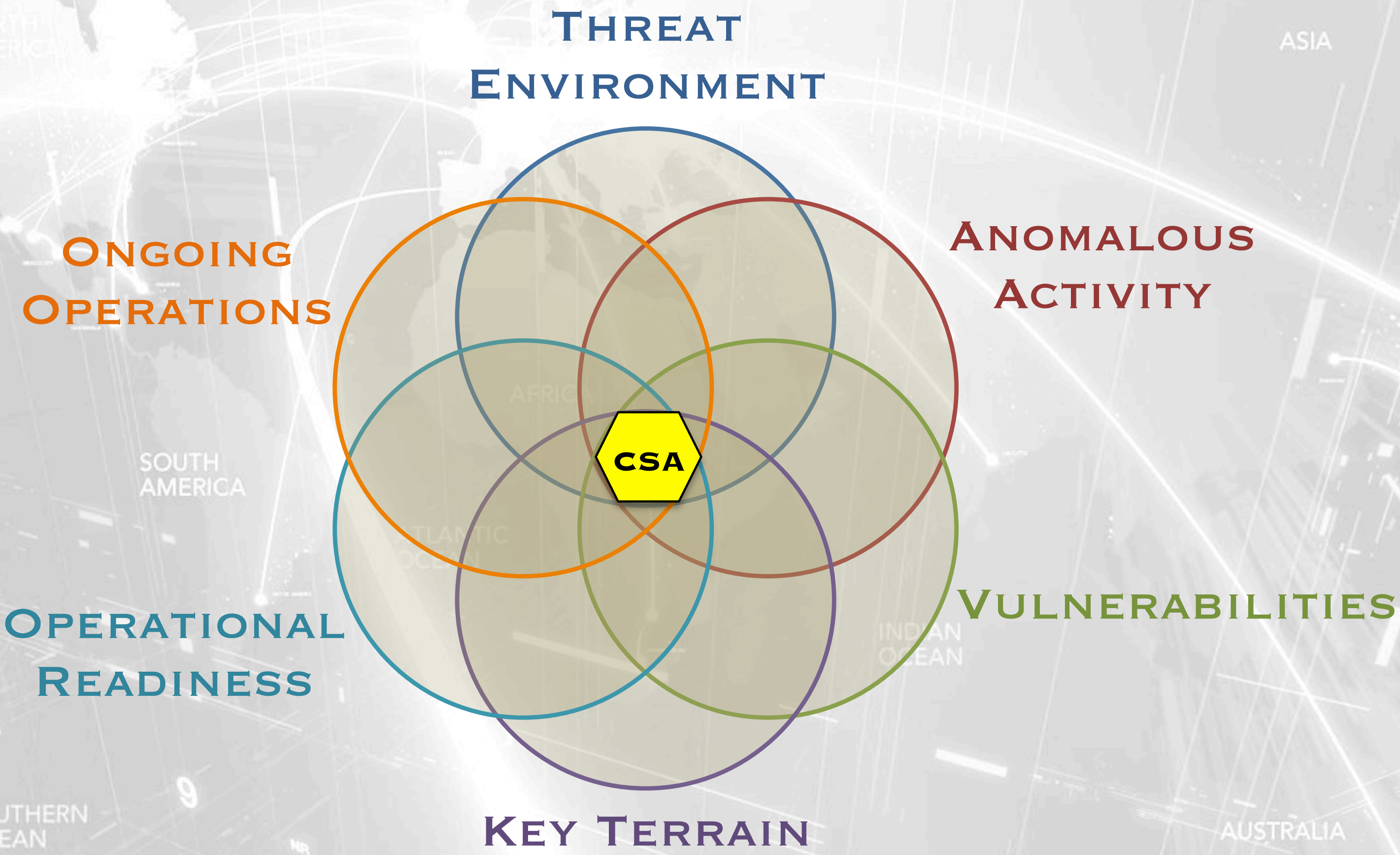
Ultimate Goal

- Maintain strategic and tactical understanding while continuously taking action or making operational risk decisions

- To allow incremental progress we must:
  - Identify decisions and actions
  - Identify and access appropriate data
  - Build analytic tools for data
  - Visualize data for decision makers

Holistic Operational Framework

CYCON '1



Threat Environment

Ongoing Operations

Anomalous Activity

CSA

Operational Readiness

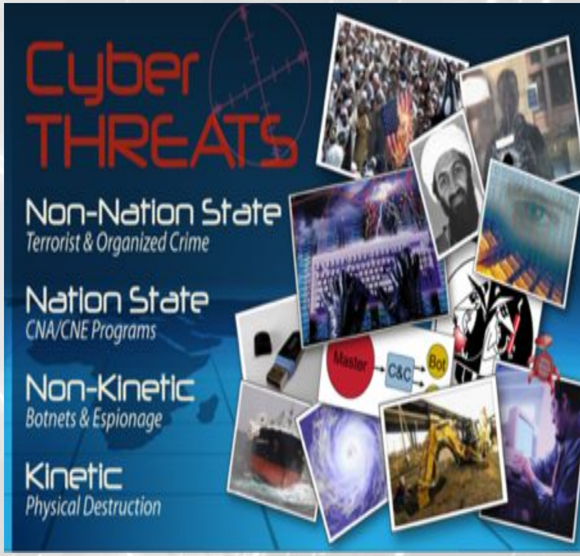
Vulnerabilities

Key Terrain

Information from all six data classes must be fused, correlated, analyzed, and visualized in near real time for optimal Cyber Situational Awareness

Threat Environment

- Identify potential attackers
- Identify the goals and objectives
- Identify the normal operations
- May reveal attackers capability and trends
- Adversary profiles leads to attribution and aligning preemptive actions

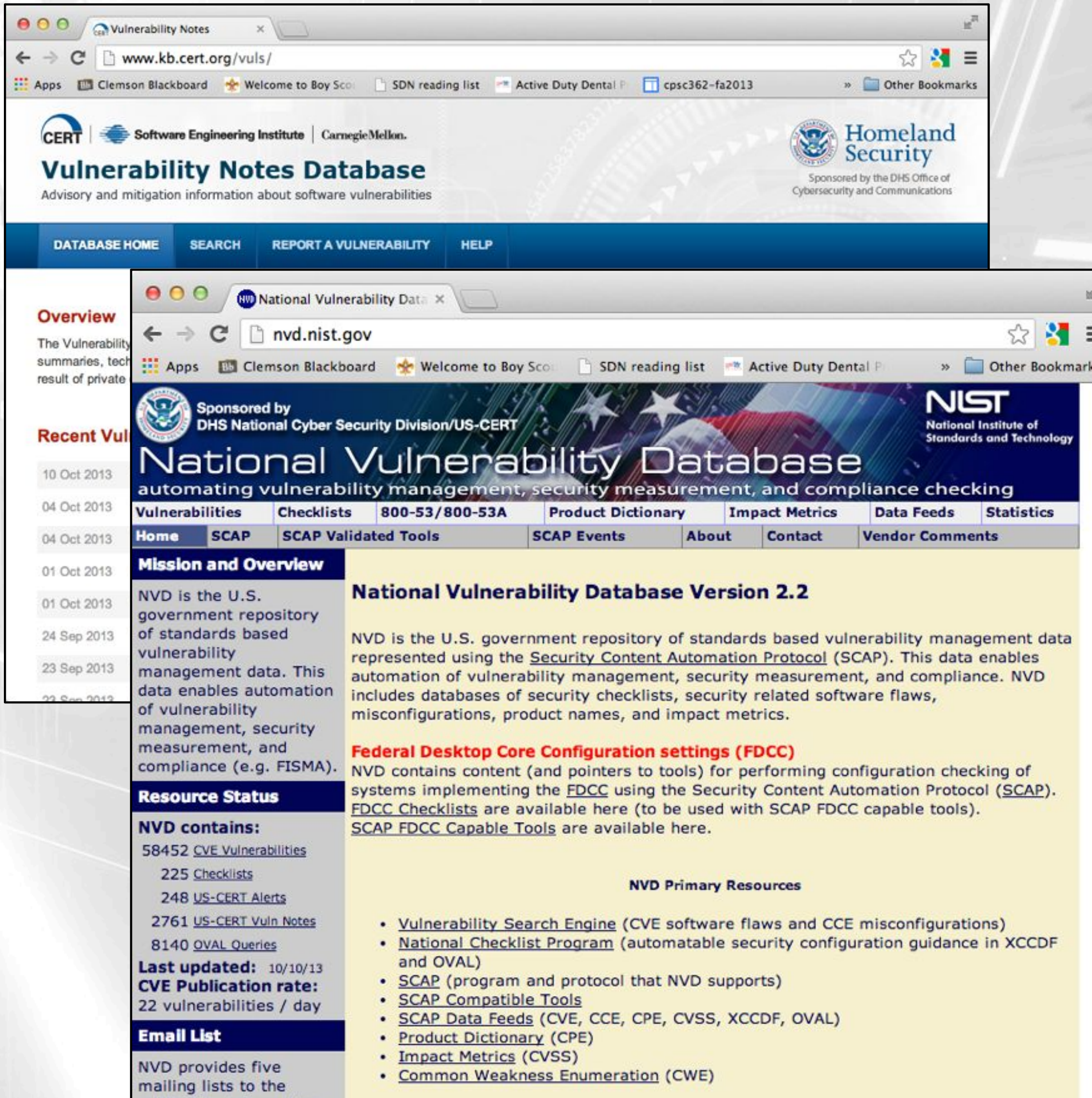


Anomalous Activity

- Firewalls, Antivirus, Intrusion detection systems detect anomalous activity
- Rules established based on known attack vectors
- Unable to detect 0-day or polymorphic exploits
- Baseline historical and current normalized data needed to identify anomalies

VULNERABILITIES

- Vulnerabilities exist in all systems
- Technology advances too rapidly for security
- Minimize vulnerabilities best option
- Must be aware of where the vulnerabilities exist in your system
- Must continuously assess



Vulnerability Notes Database

Advisory and mitigation information about software vulnerabilities

Sponsored by the DHS Office of Cybersecurity and Communications

Overview

The Vulnerability
summaries, tech
result of private

Recent Vul

10 Oct 2013
04 Oct 2013
04 Oct 2013
01 Oct 2013
01 Oct 2013
24 Sep 2013
23 Sep 2013
23 Sep 2013

Sponsored by
DHS National Cyber Security Division/US-CERT

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:
58452 CVE Vulnerabilities
225 Checklists
248 US-CERT Alerts
2761 US-CERT Vuln Notes
8140 OVAL Queries
Last updated: 10/10/13
CVE Publication rate:
22 vulnerabilities / day

Email List

NVD provides five mailing lists to the

National Vulnerability Database Version 2.2

NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

Federal Desktop Core Configuration settings (FDCC)

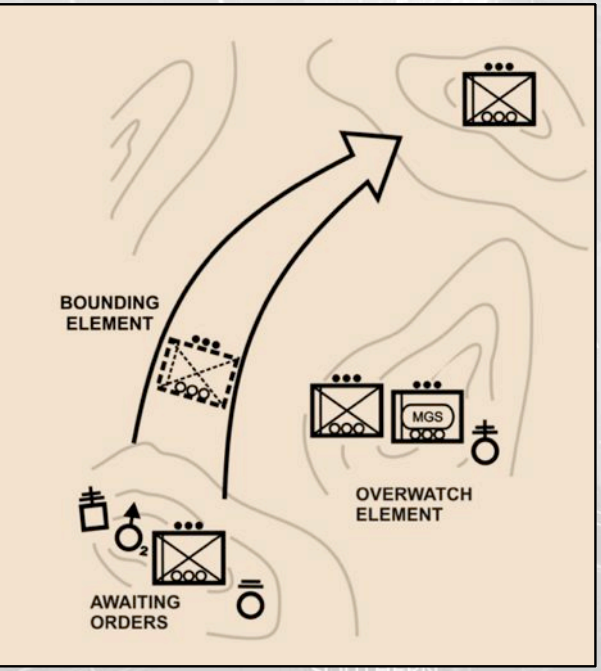
NVD contains content (and pointers to tools) for performing configuration checking of systems implementing the FDCC using the Security Content Automation Protocol (SCAP). FDCC Checklists are available here (to be used with SCAP FDCC capable tools). SCAP FDCC Capable Tools are available here.

NVD Primary Resources

- Vulnerability Search Engine (CVE software flaws and CCE misconfigurations)
- National Checklist Program (automatable security configuration guidance in XCCDF and OVAL)
- SCAP (program and protocol that NVD supports)
- SCAP Compatible Tools
- SCAP Data Feeds (CVE, CCE, CPE, CVSS, XCCDF, OVAL)
- Product Dictionary (CPE)
- Impact Metrics (CVSS)
- Common Weakness Enumeration (CWE)

Key Terrain

- Organizations have numerous, geographically-dispersed systems
- Full knowledge of all systems is impractical
- Must identify key and prioritized cyber systems
- Allows for understanding of operational and technical risk
- Allows for prioritized defense



Operational Readiness

- Must know the readiness and capability of cyber forces and assets
- The OR of a cyber force includes
  - Readiness of its tools and capabilities
  - Training and availability of its operators
  - Integrity of network sensors, paths and systems
- Must understand mission dependencies
- Leads to realization of impact of cyber events

Ongoing Operations

- Status of all ongoing kinetic and cyber operations must be considered
- Deconflict controlled outages and upgrades
- Dynamic changes in key terrain
- Adjust defensive procedures for certain timeframes
- Reallocate assets to support upcoming missions

Operational Case Study

- Emphasize the value of holistic fusion of data from all six classes

- A commander and staff make more informed decisions the closer they are to the intersection of all six classes

- Decision making process improves as additional classes of information are considered

Joint Task Force (JTF)

- Joint Task Force– Ad hoc military organization formed to accomplish a specific task

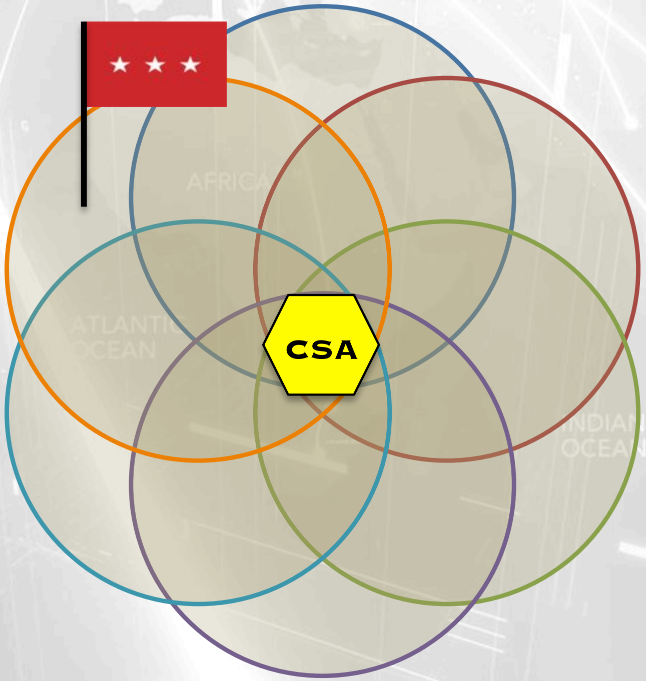
- Theoretical JTF is conducting missions requiring continuous flow of logistics and personnel into area of operations

FUNNY OR DIE
VIRAL SHORES
BRITNEY
MARU GULF
MUSIC VIDEO BAY
RICK ROLLING HILLS (DESERTED)
YOUTUBE
HTML5 SWAMP
VIMEO
YELP
ISLE OF TEENAGERS WHO JUST DISCOVERED MACROECONOMICS
SOCIAL MEDIA CONSULTANT CHANNEL
GOOGLE
GEOCACHES
GEOTAGGED
FOURSQUARE
WEB 3.0 (UNDER CONSTRUCTION)
JOURNALISTS TRYING TO FIND THE CUTTING EDGE
BIEBER BAY
DIGG
LIFEBOATS
STUMBLEUPON
MEFI
TROLL BAY
BIT.LY MOUNTAINS
HASHTAG GAMES WHOSE POPULARITY CONFUSES AND DEPRESSES YOU
TWITTER
IRC IS
USENET (STILL HERE?!)
ICQ
SEA OF OPINIONS
CLUELESS POLITICIAN COAST
DESERT OF FOOD UPDATES
BREAKING! WAVES
PROTOCOL DIFFUSION

Commander’s SA Picture

CYCON ‘14

JTF Operations



Threat Environment

Anomalous Activity

Vulnerabilities

Key Terrain

Operational Readiness

Ongoing Operations

Pre Operations

- JTF Commander designates the Logistic Support System as key cyber terrain
  - Unclassified system on Internet, connects to commercial shipping and airflow systems
- Network sensors protecting system are degraded and require maintenance scheduled in two months
- Proficient cyber investigation and forensic unit attending commercial certification training in US

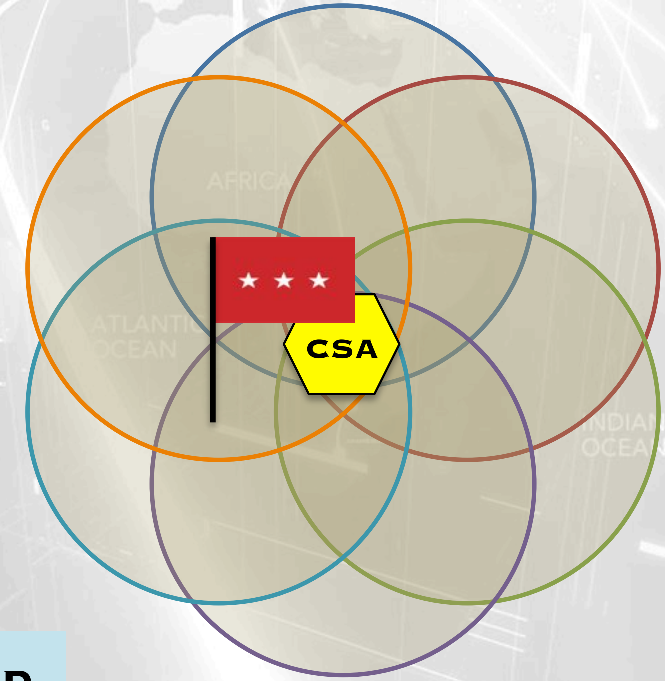
Commander’s SA Picture

Threat Environment

JTF Operations

Ongoing Operations

Anomalous Activity



Operational Readiness

Vulnerabilities

Cyber unit at training

Degraded Network Sensors

Key Terrain

During Operations [1 of 3]

- Critical vulnerability in logistic support system is discovered
- Potential patch not available for 30 days due to required testing with legacy OS
- Vulnerability allows root level access which could lead to implant of malicious software on unpatched systems
- Commander is advised, decides to take no action at this time

Commander’s SA Picture

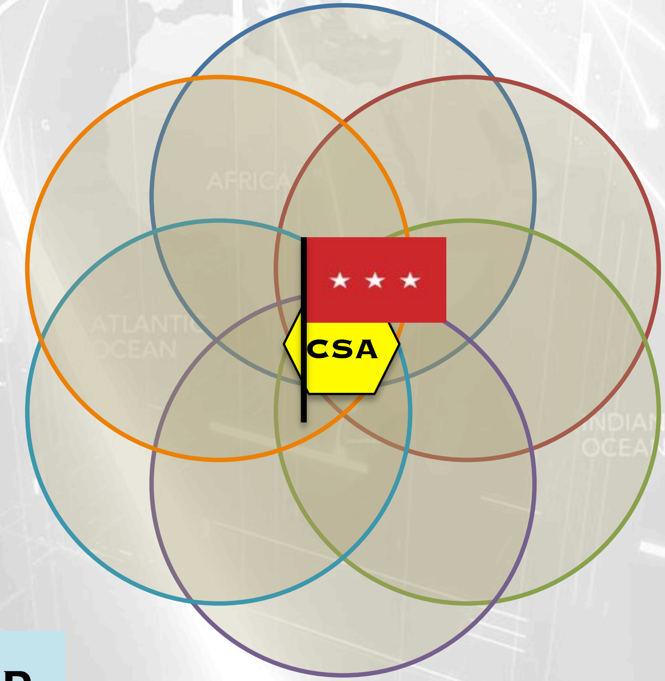
CYCON ‘14

JTF Operations

Ongoing Operations

Threat Environment

Anomalous Activity



Operational Readiness

Cyber Unit At Training

Degraded Network Sensors

Vulnerabilities

Unpatched Root Level Access, Allows Malware Implant

Key Terrain

During Operations [2 of 3]

- Cyber alert is released, reports adversary has increased interest in disrupting and influencing logistical flow
- Known to deploy Trojan-horse type software on susceptible systems
- Commander decides to recall cyber force from training and refocus on monitoring the logistics systems

Commander's SA Picture

CYCON '14

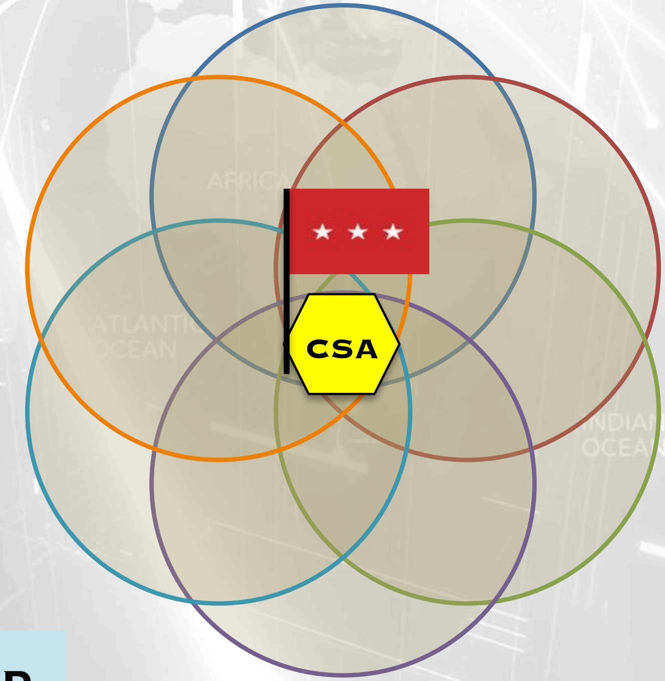
Adversary Increased Interest in Disrupting Logistics, Employs Trojan horse tactics

Threat Environment

JTF Operations

Ongoing Operations

Anomalous Activity



Operational Readiness

Cyber Unit At Training

Degraded Network Sensors

Vulnerabilities

Unpatched Root Level Access, Allows Malware Implant

Key Terrain

During Operations [3 of 3]

- Team discovers anomalous behavior in logistical support systems

- Over half the systems are sending irregular sized traffic over the same TCP port to and IP subnet outside of the US

- Forensics determine documents are being slowly exfiltrated over covert channels

Commander’s SA Picture

Adversary Increased Interest In Disrupting Logistics, Employs Trojan Horse Tactics

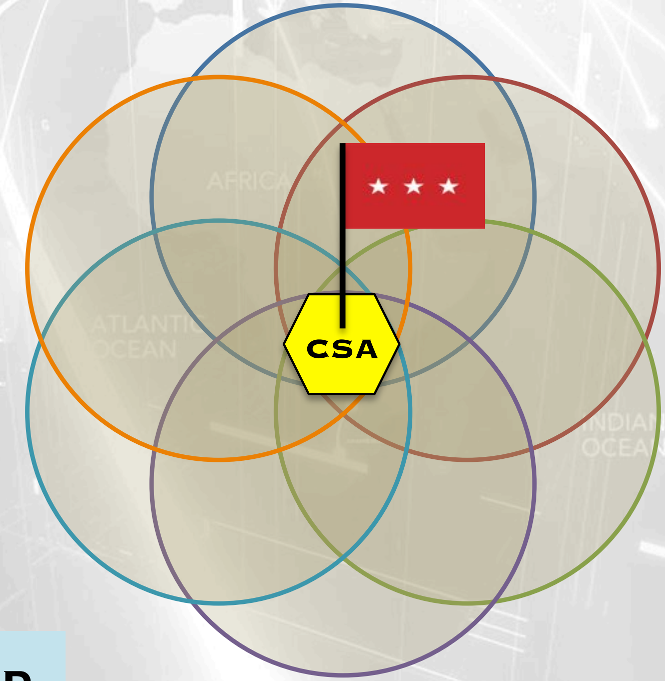
Threat Environment

Irregular TCP transmissions to non-US IP space

Anomalous Activity

JTF Operations

Ongoing Operations



Operational Readiness

Cyber unit at training

Degraded network sensors

Vulnerabilities

Unpatched Root Level Access, Allows Malware Implant

Key Terrain

Commanders Actions

- Initiates crisis action planning
- Requests immediate upgrade to sensor platforms
- Directs removal of logistical support system from network
- Request detail forensics investigation into which files were stolen to assess operational impact
- Relocated naval and air assets to protect shipping and personnel movements
- Directs daily updates from cyber forces

Case Study Summation

- Case Study:
  - All SA classes have abundant information
  - Data is available for consumption by integrated systems or motivated individual
- Reality:
  - Cyber forces don’t concern themselves with ongoing operations
  - Commanders don’t understand cyber key terrain
  - Operational Readiness of cyber forces not understood
  - Vulnerability, threat, and anomalous activity is presented as technical jargon to decision makers

Challenges

- Numerous challenges exist
  1. Organizational Fear
  2. Data Consolidation/Normalization
  3. Data Synthesis
  4. Visualization and Dissemination
  5. Timeliness
- Key barriers involves organizational and technical challenges

Conclusion

- Robust situational awareness of the cyber environment is absolutely critical to cyber defense operations
- Holistic Operational Framework integrates information from six data classes
- Enables commanders and leaders to incorporate cyberspace into decision making process

QUESTIONS?

Acknowledgements: Thanks to Triiip Bowen, Jason Koepke, and Rob Schrier