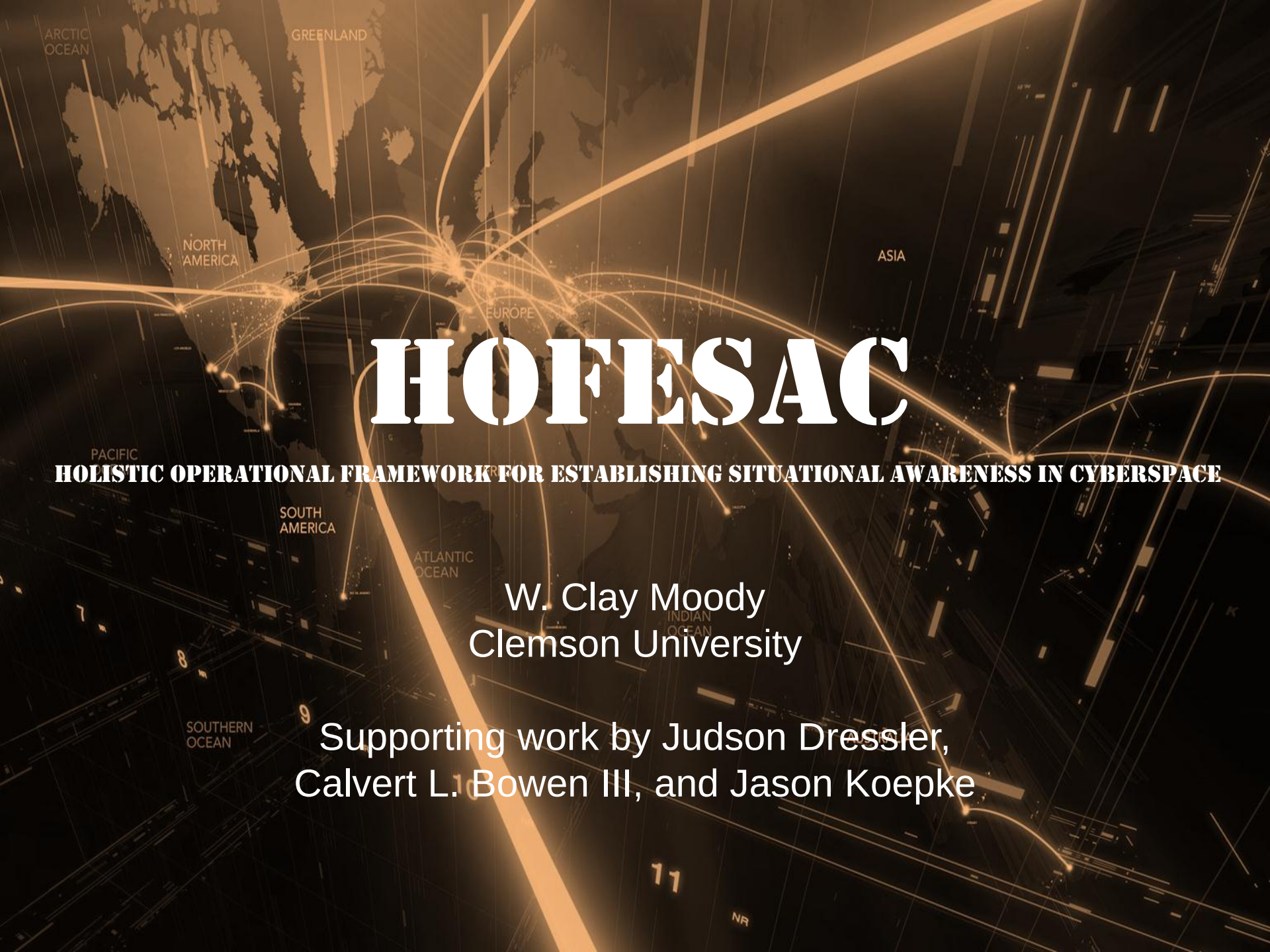


HOFESAC

HOLISTIC OPERATIONAL FRAMEWORK FOR ESTABLISHING SITUATIONAL AWARENESS IN CYBERSPACE

W. Clay Moody
Clemson University

Supporting work by Judson Dressler,
Calvert L. Bowen III, and Jason Koepke

Disclaimer

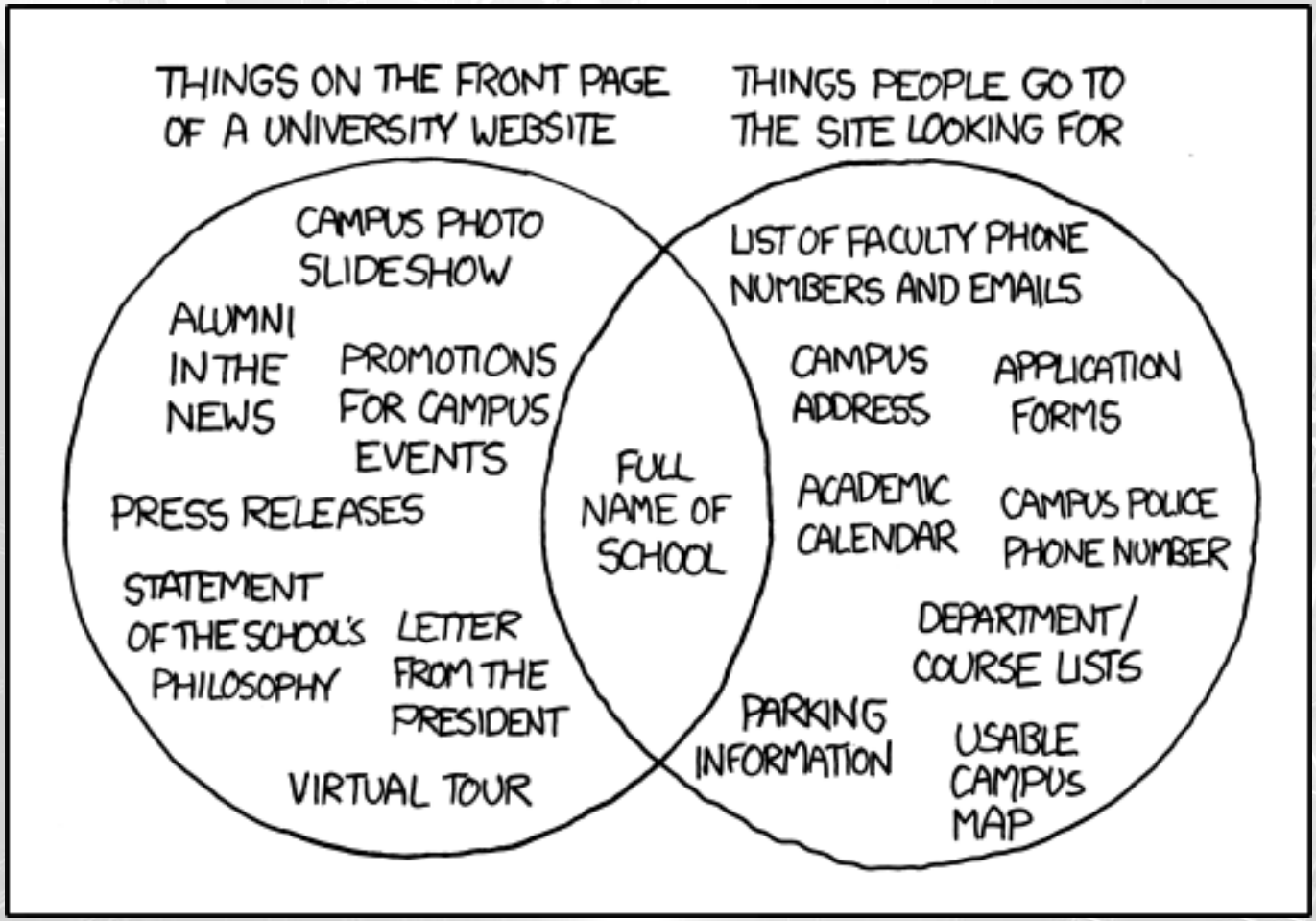
- The views and opinions expressed in this presentation are those of the authors and do not necessarily reflect those of Clemson University, the United States Military Academy, United States Cyber Command, or the United States Army

- 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?



Introduction

- National critical infrastructure has key role in:

Energy

Finance

Transportation

Defense

- Disruption of US DoD systems significantly damages ability to defend the nation

- Must understand the cyber operating environment to secure the nation

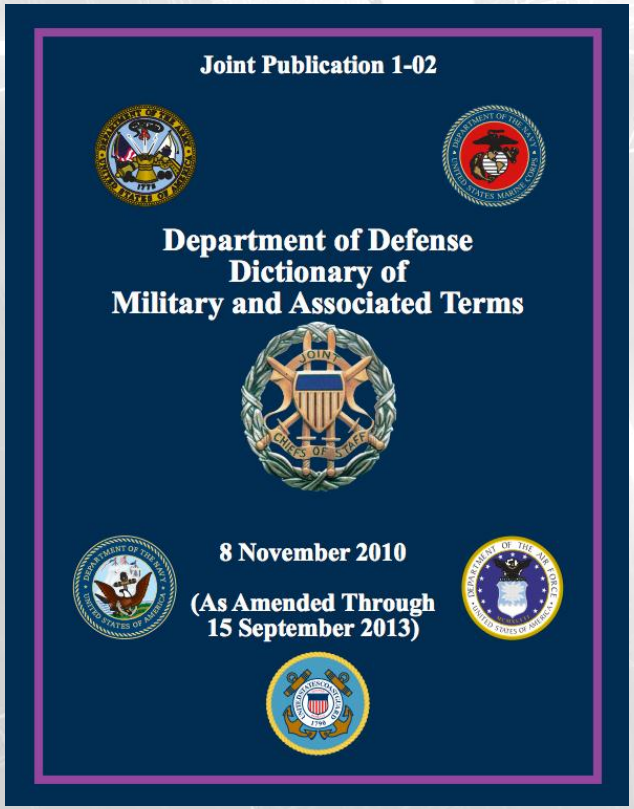
The View from the Top

- "The United States is fighting a **cyber-war** today, and we are losing. It's that simple. As the most wired nation on Earth, we offer the most targets of significance, yet our **cyber-defenses are woefully lacking**."
  - *Former Director of the NSA, Mike McConnell – Washington Post Feb 2010*

- "... to defend those networks and make **good decision** in exercising operational control over them ... will require much **greater situational awareness** and **real-time visibility** of intrusions into our networks."
  - *Commander, United States Cyber Command (USCYBERCOM) and current Director of the NSA General Keith Alexander – Congressional Testimony 2010*

Pictures – Courtesy of Wikipedia : Emphasis added

Cyberspace doctrine



- 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

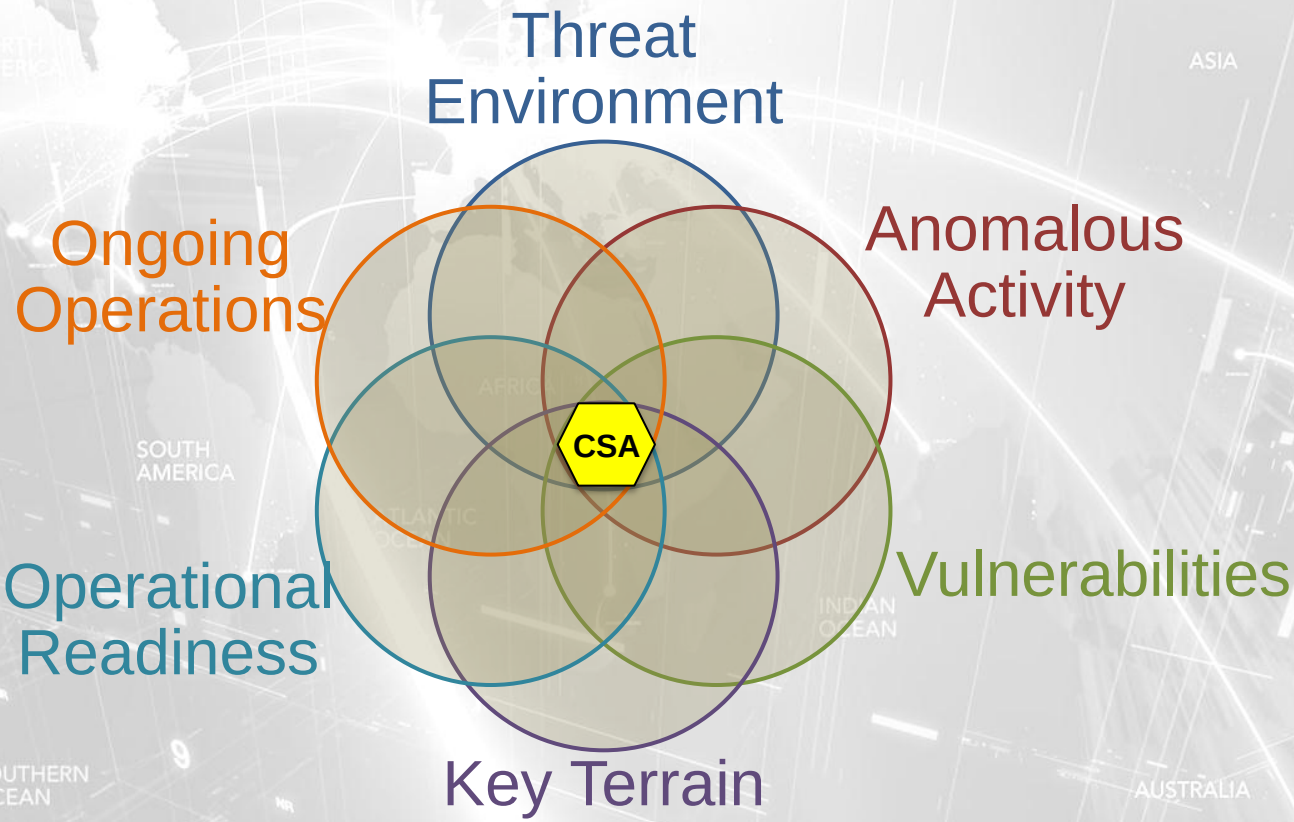
"Knowledge and understanding of the operational area's environment, factors, and conditions, to include the status of friendly and adversary forces, neutrals and noncombatants, weather and terrain, that enables timely, relevant, comprehensive, and accurate assessments, in order to successfully apply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

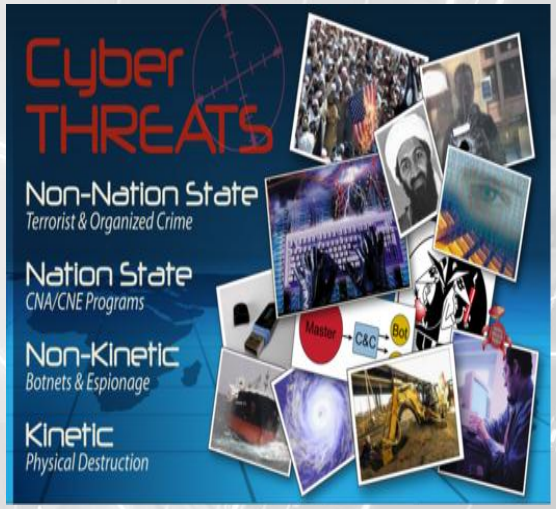
Holistic Operational Framework



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



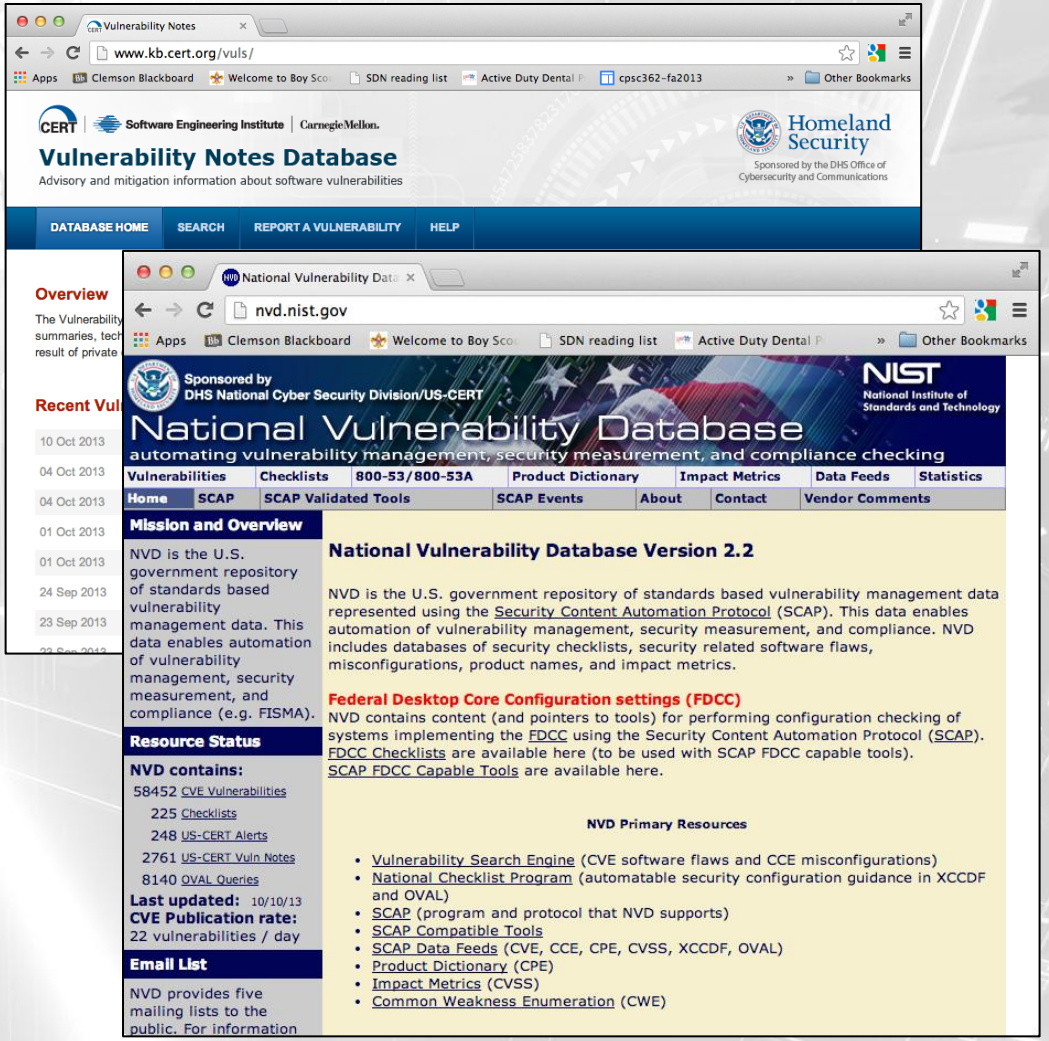
- May reveal attackers capability and trends
- Adversary profiles leads to attribution and aligning preemptive actions

Anomalous Activity

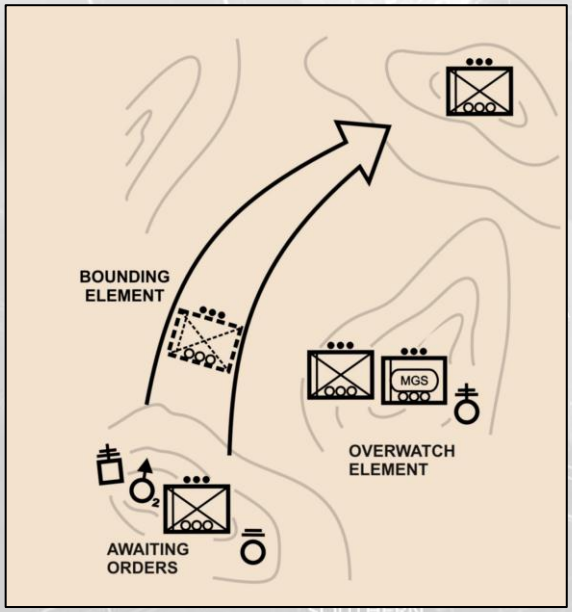
- Firewalls, Antivirus, Intrusion detection systems detect anomalous activity
- Rules established based on known attack vectors
- Unable to detect 0-day or polymorphic exploits
- Baseline historical and current normalized data needed to identify anomalies

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 system for vulnerabilities



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

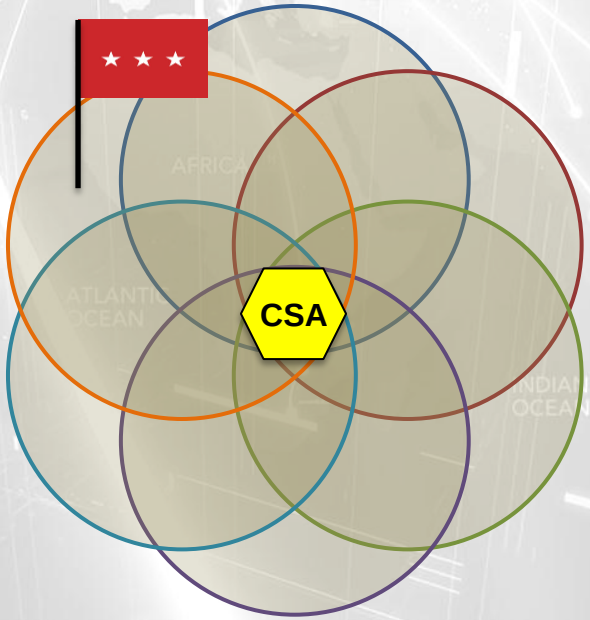
- Theoretical JTF is conducting missions requiring continuous flow of logistics and personnel into area of operations

Commander's SA Picture

Threat Environment

JTF Operations

Ongoing Operations



Anomalous Activity

Operational Readiness

Vulnerabilities

Key Terrain

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

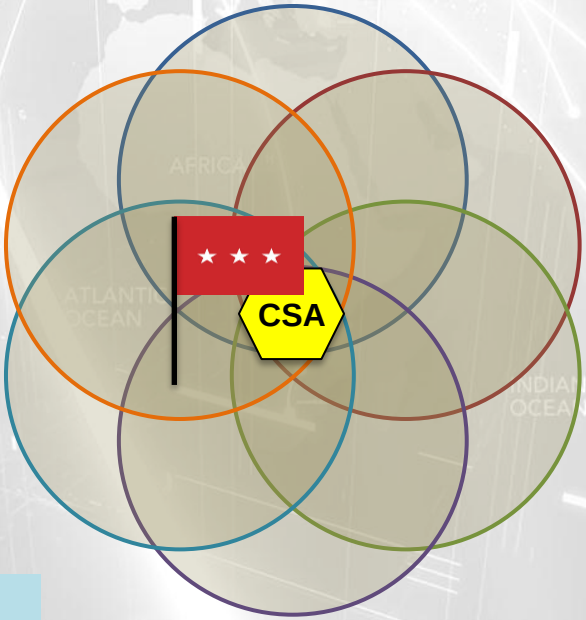
Commander's SA Picture

Threat Environment

JTF Operations

Ongoing Operations

Anomalous Activity



Operational Readiness

Vulnerabilities

CYBER UNIT AT TRAINING

Degraded Network Sensors

Key Terrain

Logistical System

During Operations [1 of 3]

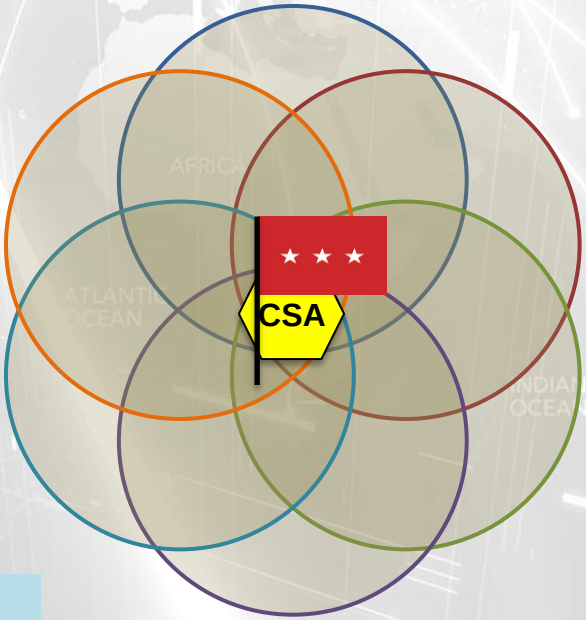
- Critical vulnerability in logistic support system is discovered
- Potential patch not available for 30 days due to required testing with legacy OS
- Vulnerability allows root level access which could lead to implant of malicious software on unpatched systems
- Commander is advised, decides to take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

Commander's SA Picture

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

Logistical System

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

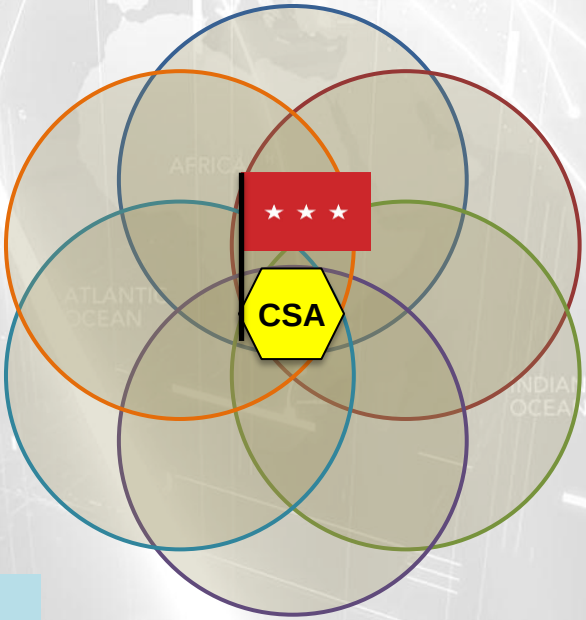
Commander's SA Picture

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

Logistical System

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

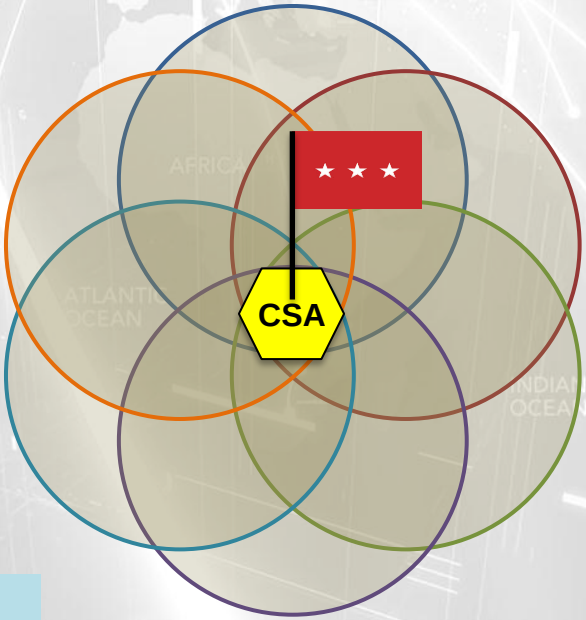
Threat Environment

JTF Operations

Irregular TCP transmissions to non-US IP space

Ongoing Operations

Anomalous Activity



Operational Readiness

Cyber unit at training

Degraded network sensors

Vulnerabilities

Unpatched Root Level Access, Allows Malware Implant

Key Terrain

Logistical System

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

- Cyber SA requires data and information to be collected, analyzed, and displayed to user in timely and relevant manner
- Numerous challenges exist
- Key barrier involves organizational and technical challenges

Challenge 1: Organizational Fear

- Gaining access to data can lead to turf war

- Organizations fear giving access to their data
  - Humiliation in revealing security flaw
  - Losing a competitive edge or public confidence
  - Creation of "1,000 mile screwdriver" from higher

- Fear prevents complete Cyber SA

- Must define and enforce a single data owner to aggregate data for analysis

Challenge 2: Data Consolidation / Normalization

- Data collected by humans and automated systems
- Ingesting all data currently impractical
- Potential in future with cloud computing and increased network bandwidth
- Must determine the proper metrics and alert thresholds
- Data must be consolidated and normalized according to standardized formats

Challenge 3: Data Synthesis

- Stove-piped solutions exist today
- Must fuse stove-piped solutions together with advanced processing algorithms
- Establish baseline network activity
- Move away from signature based detection
- Discover disparate attacks across geographical separated network

Challenge 4: Viz and Dissemination

- Human intervention will be required until true machine-to-machine detection
- Rapid human understanding through visual presentation of data
- Geographical (norm) versus logical or temporal view
- Dissemination plan must be established to get information to right user within proper authorities and permissions

Challenge 5: Timeliness

- Increase of false positives and decrease of accuracy hamper timely response
- Cyber attacks occur within milliseconds
- Summarize vast amounts of data and delivered in a timely fashion

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 Judd Dressler, Triiip Bowen, Jason Koepke, Rob Schrier and Greg Conti