A Need for Tactics, Techniques, and Procedures (TTP)

Mr. Frank Honkus

USCYBERCOM J53 ICS SME

Joint Base Architecture for Secure ICS (J-BASICS) Joint Test Technical Advisor

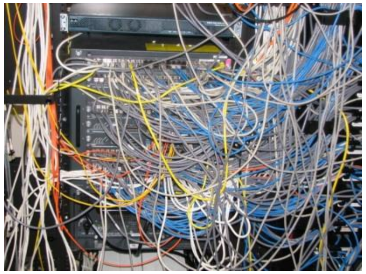
The overall classification of this briefing is: **UNCLASSIFIED**

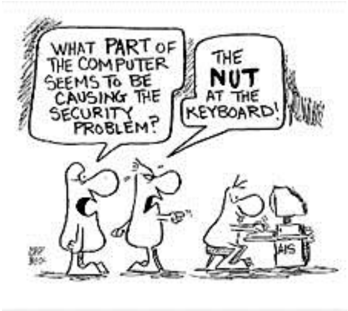
The Situation

- Adversaries appear determined to penetrate US critical infrastructure

- If Plan A of the adversary to penetrate your network does not work they have 25 more letters of the alphabet to try

-




WHAT PART OF THE COMPUTER SEEMS TO BE CAUSING THE SECURITY PROBLEM?
THE NUT AT THE KEYBOARD!
AIS

- As a result there is a good chance ICS networks are going to be penetrated and attacked

The threat, coupled with the cybersecurity challenges and long life span on ICS equipment creates ***ideal*** conditions for a cyber attack

The Evolution of the Threat

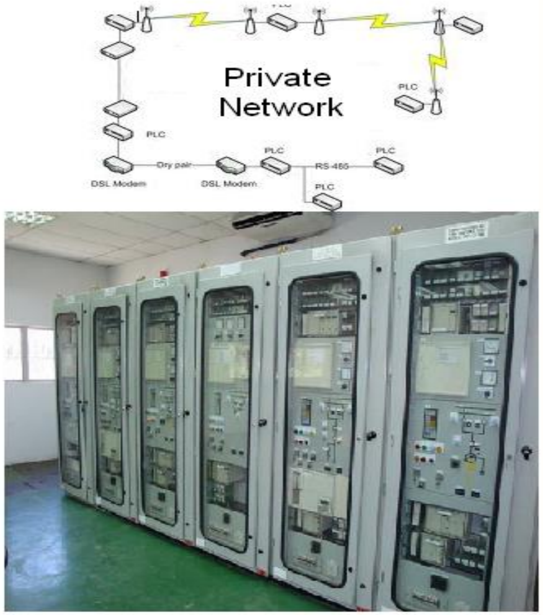
Advanced Nation-State Level Hacking Tools Proliferating

PAST

Minimal Threat Environment

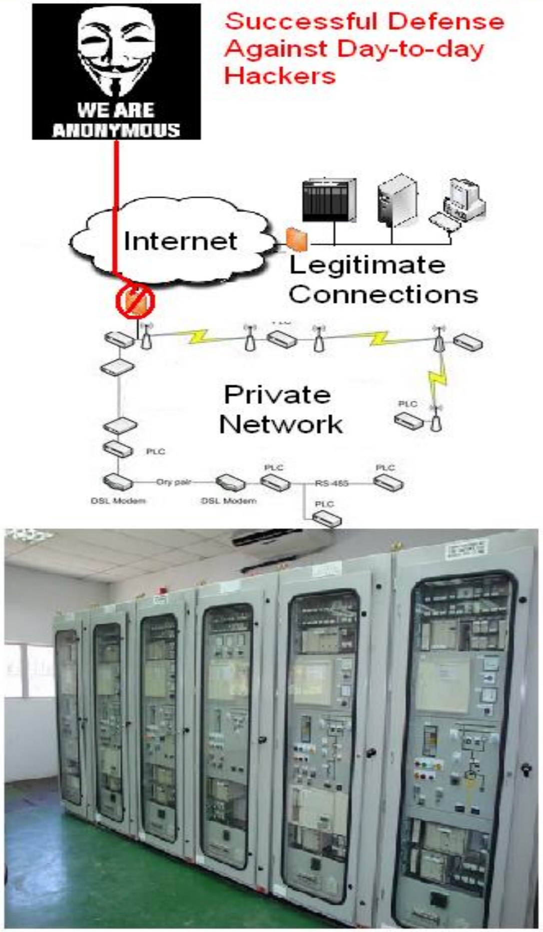
No Internet Connection

Individual Hackers & Nation States: No Cyber Attack Capability



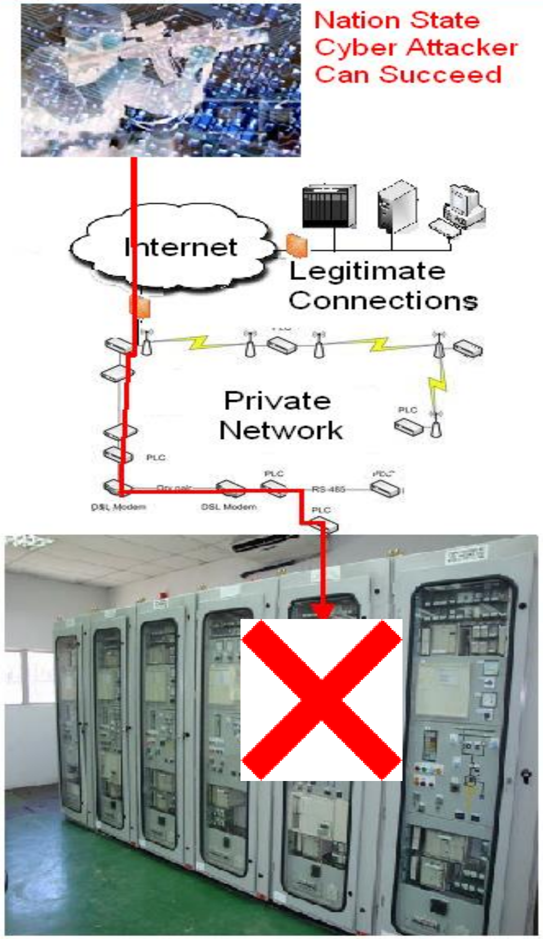
Critical Control System Component

Present



Successful Defense Against Day-to-day Hackers

Critical Control System Component



Nation State Cyber Attacker Can Succeed

Critical Control System Component

The endpoint ICS devices have a long life span.

Siege Warfare – Has it ever Worked for the Defender?

Today – <u>DODIN Operations</u>

1992 -1996 - Sarajevo

1954 – Dien Bien Phu

Yorktown - 1781

1940 - Maginot Line

Today DoDIN

1574 - Leiden

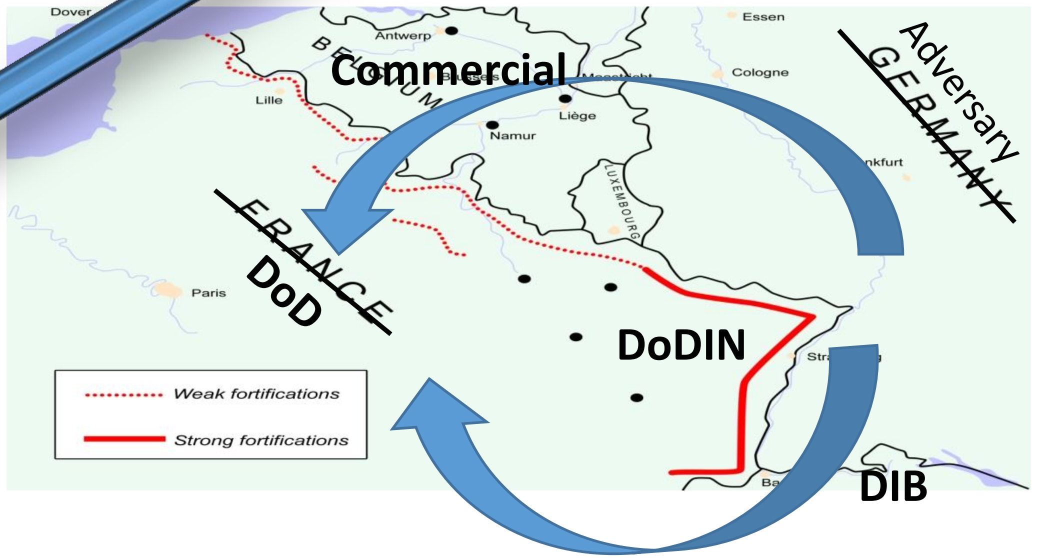
1099 - Jerusalem

717-718 - Constantinople

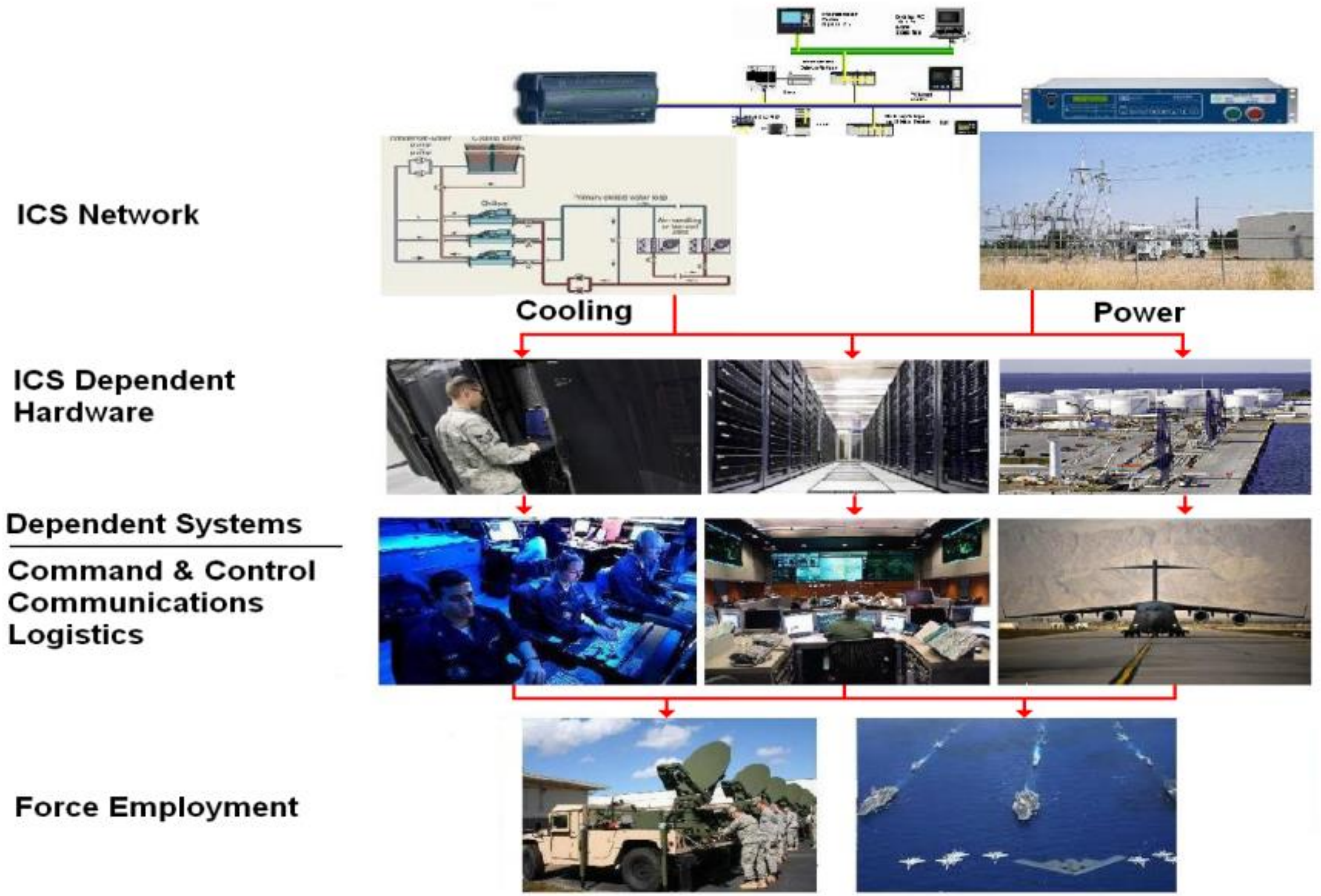
52 B.C. - Alesia

149-146 B.C. - Carthage

1194-1184 B.C. - Troy



Why ICS Matters: DoD Mission - To Fight and Win



ICS Network

Cooling

Power

ICS Dependent Hardware

Dependent Systems

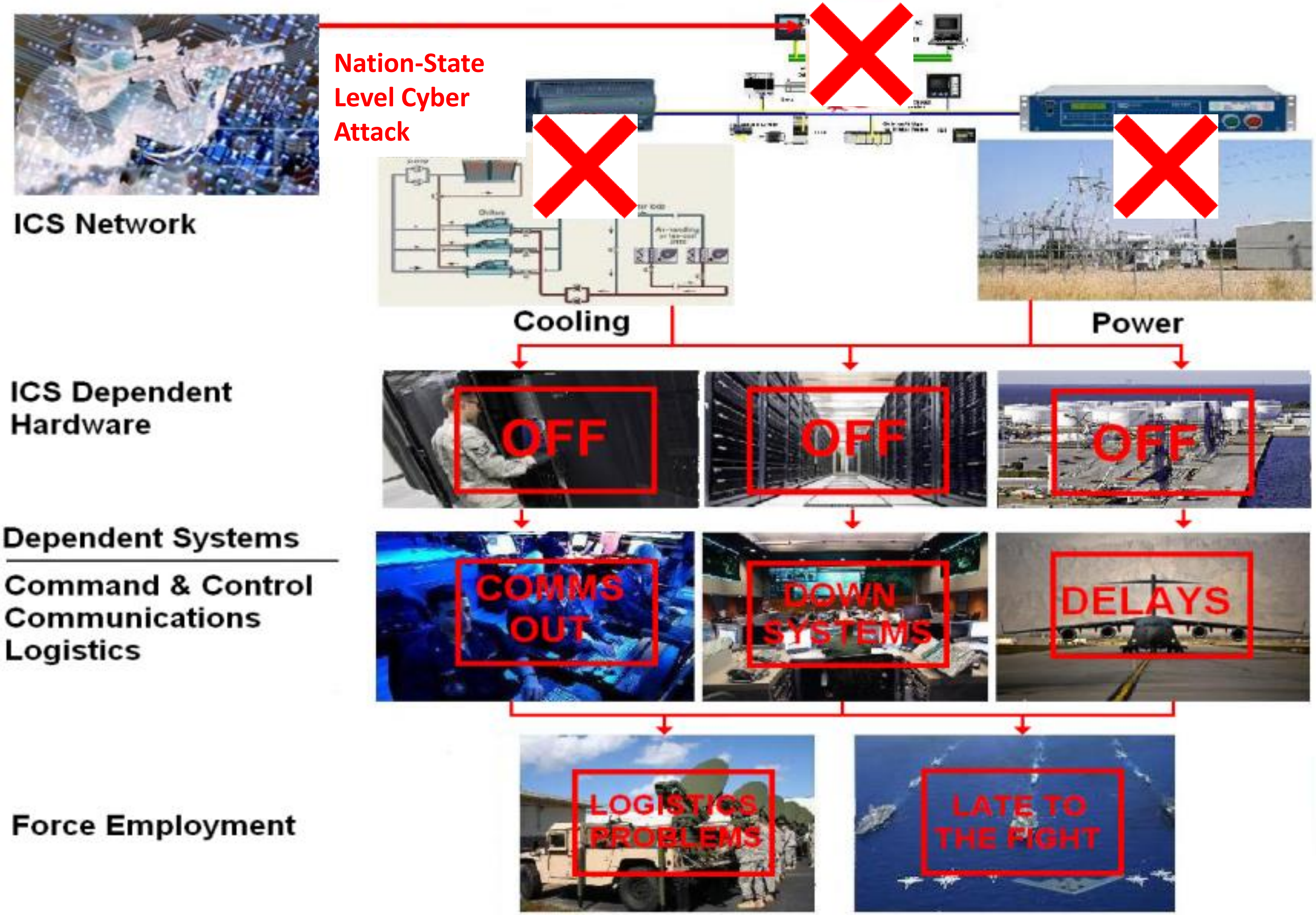
Command & Control
Communications
Logistics

Force Employment

ICS – Where Cyber can ***physically*** alter the Battlespace

Impact on Force Projection

Tasks Require Information



Nation-State Level Cyber Attack

ICS Network

Cooling

Power

ICS Dependent Hardware

Dependent Systems

Command & Control
Communications
Logistics

Force Employment

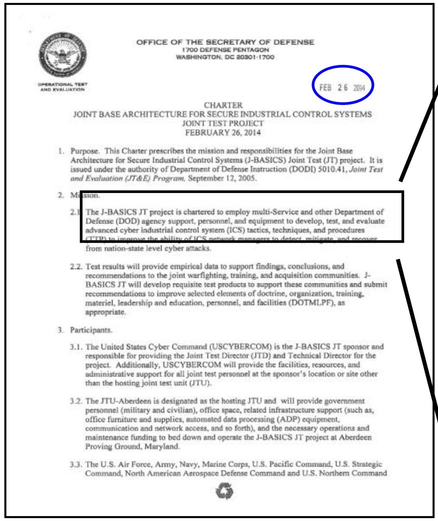
A Solution

“Resilient” defensive techniques are more effective in ICS environments

Joint Base Architecture for Secure Industrial Control Systems (J-BASICS) Joint Test

J-BASICS

Charter



OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

FEB 26 2014

CHARTER
JOINT BASE ARCHITECTURE FOR SECURE INDUSTRIAL CONTROL SYSTEMS
JOINT TEST PROJECT
FEBRUARY 26, 2014

1. Purpose. This Charter prescribes the mission and responsibilities for the Joint Base Architecture for Secure Industrial Control Systems (J-BASICS) Joint Test (JT) project. It is issued under the authority of Department of Defense Instruction (DODI) 5010.41, *Joint Test and Evaluation (JT&E) Program,* September 12, 2005.

2. Mission.

2.1. The J-BASICS JT project is chartered to employ multi-Service and other Department of Defense (DOD) agency support, personnel, and equipment to develop, test, and evaluate advanced cyber industrial control system (ICS) tactics, techniques, and procedures (TTP) to improve the ability of ICS network managers to detect, mitigate, and recover from nation-state level cyber attacks.

2.2. Test results will provide empirical data to support findings, conclusions, and recommendations to the joint warfighting, training, and acquisition communities. J-BASICS JT will develop requisite test products to support these communities and submit recommendations to improve selected elements of doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF), as appropriate.

3. Participants.

3.1. The United States Cyber Command (USCYBERCOM) is the J-BASICS JT sponsor and responsible for providing the Joint Test Director (JTD) and Technical Director for the project. Additionally, USCYBERCOM will provide the facilities, resources, and administrative support for all joint test personnel at the sponsor's location or site other than the hosting joint test unit (JTU).

3.2. The JTU-Aberdeen is designated as the hosting JTU and will provide government personnel (military and civilian), office space, related infrastructure support (such as, office furniture and supplies, automated data processing (ADP) equipment, communication and network access, and so forth), and the necessary operations and maintenance funding to bed down and operate the J-BASICS JT project at Aberdeen Proving Ground, Maryland.

3.3. The U.S. Air Force, Army, Navy, Marine Corps, U.S. Pacific Command, U.S. Strategic Command, North American Aerospace Defense Command and U.S. Northern Command

FEB 26 2014

"employ multi-Service and other Department of Defense (DoD) agency support, personnel and equipment to develop, test, and evaluate advanced cyber industrial control system (ICS) tactics, techniques, and procedures (TTP) to improve the ability of ICS network managers to detect, mitigate, and recover from nation-state level cyber attacks"

Lead Sponsor

USCYBERCOM

Operational Endorsers

NORAD-NORTHCOM
OASD (AT&L)/EI&E
USPACOM
USSTRATCOM

Background

The Joint Base Architecture for Secure Industrial Control Systems (J-BASICS) is an OSD funded, Army Test and Evaluation managed, Joint Test to develop defensive cyber TTPs to detect, mitigate, and Recover ICS/SCADA from nation-state level of cyber attacks.

The Joint Test was chartered in 2014 and is scheduled for closedown on or before 31 Dec 2015.

Problem Statement

Network managers supporting DOD Industrial Control Systems (ICS) lack TTP to detect, mitigate, and recover from nation-state level cyber attacks.

Tactics, Techniques & Procedures

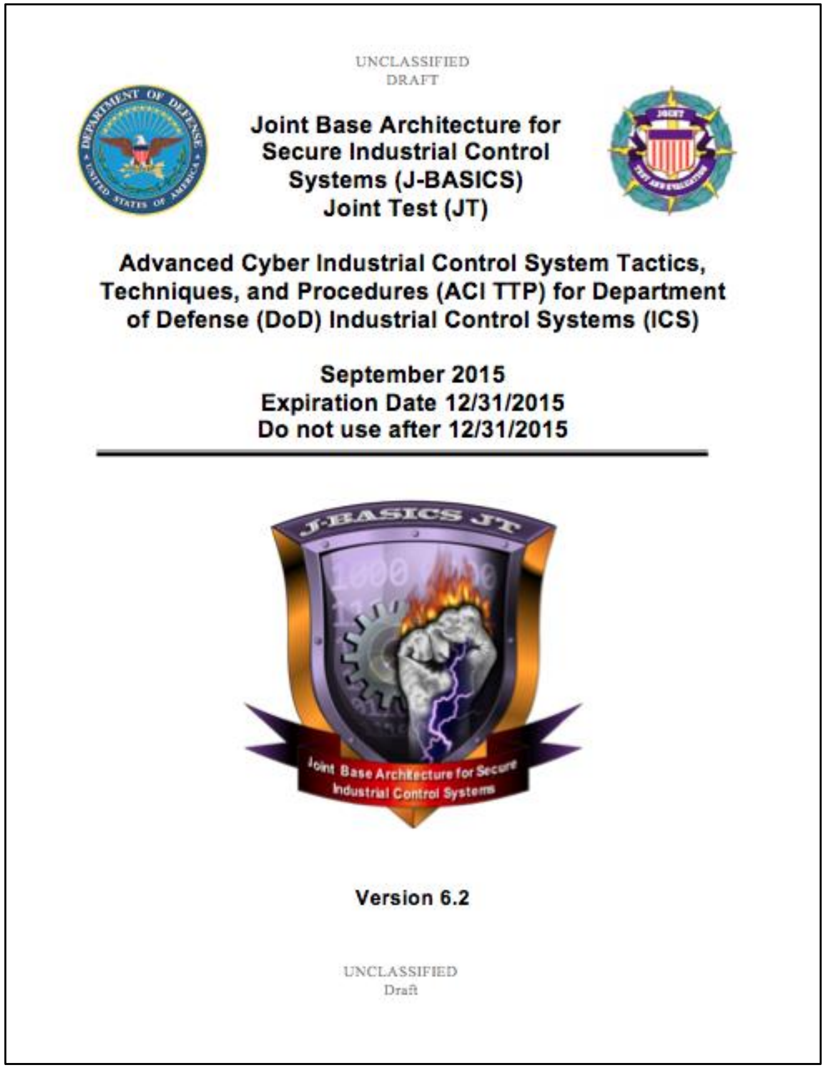
- **Key Considerations**
  - The TTP must complement existing policies and procedures
  - The TTP must fill cyber incident response gaps for ICS
  - The TTP must be effective, usable, and applicable to the warfighter’s ICS environment
  - The TTP must be scalable and able to adapt to future requirements

- **Related Policy & Guidance**
  - CJCSM 6510.01B: Defense Cyber Incident Handling
  - DoDI 8510.01: Risk Management Framework
  - NIST SP800-53: Security & Privacy Controls for Federal Information Systems
  - CNSSI No. 1243: Security Control Overlays for ICS
  - NIST SP800-37: Applying RMF to IT Security Life Cycle
  - NIST SP800-82: ICS Security

Tactics, Techniques & Procedures

- **Methodology Approach**
  - Research existing studies on cyber security procedures in ICS
    - Air Force Institute of Technology (AFIT)
    - Naval Postgraduate School
    - MITRE Cyber Resiliency Metrics
    - Technical Reference – Industrial Network Security, Handbook of SCADA, etc
  - Conduct four site surveys to gather information on existing ICS operations
    - Kitsap Naval Base
    - Joint Base Lewis-McChord
    - Ft Carson Army Base
    - Wright-Patterson Air Force Base
  - Develop TTP to integrate with ICS work flow

Tactics, Techniques & Procedures



UNCLASSIFIED
DRAFT

Joint Base Architecture for Secure Industrial Control Systems (J-BASICS) Joint Test (JT)

Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of Defense (DoD) Industrial Control Systems (ICS)

September 2015
Expiration Date 12/31/2015
Do not use after 12/31/2015

J-BASICS JT
Joint Base Architecture for Secure Industrial Control Systems

Version 6.2

UNCLASSIFIED
Draft

- Three Main Sections:
  - Detect
  - Mitigate
  - Recover

Understanding Detection

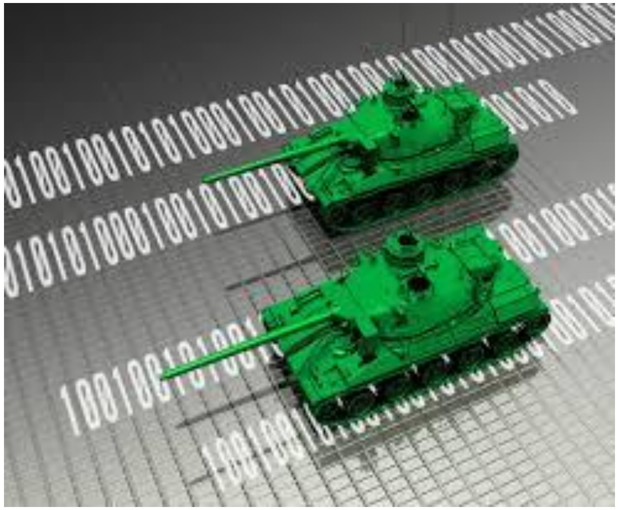
- The Detection portion of the ACI TTP enables ICS and IT operators to identify symptoms of malicious cyber activity prior to attack including:
  - System status/configuration changes
  - Unauthorized network access
  - Network traffic anomalies
  - Initial mode(s) of access
  - Lateral network movement
  - Network hop points
  - Firmware compromise

Understanding Detection

- The key is early detection
  - Detecting the enabling functions
- Evidence and IOCs determine severity level
- ICS-Specific incident escalation factors
  - What is the impact?
    - Impact of safety of an operation
    - Impact the reliability of an operation
    - Indications of capability to achieve a large scale impact
    - Number of systems impacted by the threat
  - Where does evidence exist?
  - What is the function of the system at risk? Safety-related function? Control function? Monitoring function? Auxiliary/Support function?
  - Does evidence exist of control system traffic or data leaving the controlled/protected networks?

Understanding Mitigation

- Mitigation is the ability to fight through an attack, enabling mission to move forward, by gracefully degrading the ICS network – while maintaining mission capability
- The Role of Mitigation
  - Minimize negative impact
  - Ensure some level of capability despite attack
  - 24-Hour Survival Plan/Initial Triage
- How do you mitigate a cyber attack?
  - Graduated approach to mitigation
  - Options and Flexibility
  - Network layer or function group segmentation



Understanding Recovery

- What does it mean to recover from a cyber attack?
  - More than restoring back to proper health
    - Full system re-integration (Number of devices to reintegrate)
    - Not getting re-infected
    - Putting everything together correctly
- Recovery Process
  - Not a static process
  - Ok to move between steps based on operational goals and depends on mission and operational priorities
- Return to Routine Monitoring

Field Test 1 Overview

- Location – Sandia National Labs
- 2 Identical but separate ICS networks
- 1 Week of intensive training (Oct 2014)
- 2 Weeks of test trials (Nov 2014)
- 4 Days during Cyber Flag 15
- Concurrent network and ICS technical training

- 13 Participants from across the Services
- 6 Teams: 1 IT and 1 Facility Engineer

Field Test 2 Overview

- Location – Sandia National Labs
- 2 Identical but separate ICS networks
- 1 Week of intensive training (June 2015)
- 2 Weeks of test events (June 2015)
- 4 Days during Cyber Guard 15
- Concurrent network and ICS technical training
- 12 Participants from across the Services

  (6 Teams: 1 IT and 1 Facility Engineer)

FT-2 Test Accomplishments

	Planned	Conducted					
	Required # of FT-2 Events	FT-2 Events	CG 15 Events	Free Play Events	Total Events	Scored No Tests	Total Valid Events
Detect (AP)	23	23	11	7	41	7	34
Detect (NAP)	22	23	0	0	23	1	22
Mitigate	36	41	6	0	47	2	45
Recover	14	15	1	0	16	0	16
Totals	95	102	18	7	127	10	117

FT-2:Field Test 2
CG: Cyber Guard

AP: Adversary Present
NAP: No Adversary Present

FP: Free Play

Test Results: FT-1 and FT-2

FT-1 Issues	FT-1 Result	Trials	WEC
Detect (Adversary Present)	61%	36	40%
Detect (Normal Operations)	100%	12	70%
Mitigate	87%	31	70%
Recover	89%	18	60%

FT-2 Issue	FT-2 Results	Events	WEC
Detect (Adversary Present)	62%	36	60%
Detect (No Adversary Present)	86%	22	70%
Mitigate	71%	45	80%
Recover	94%	16	60%

Overall Results

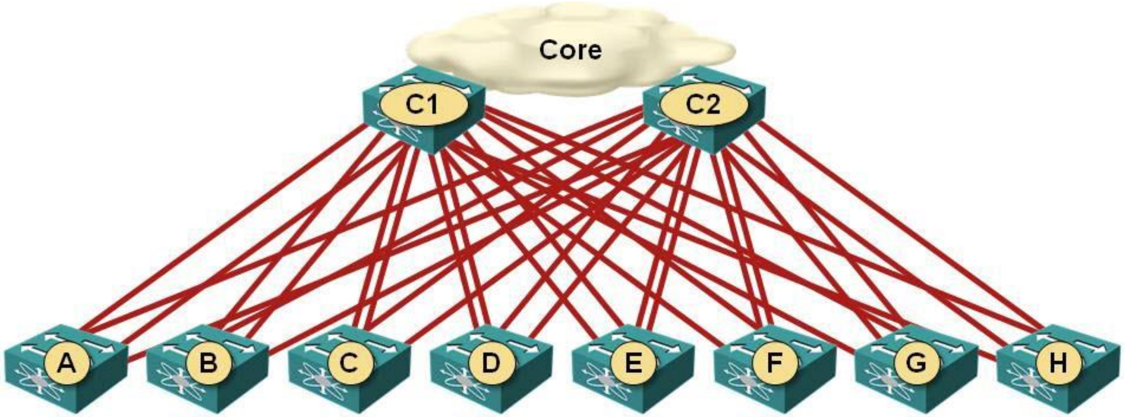
- Detect:
  - TTP allowed Operators to detect as designed. TTP was designed to:
    - Reject false positives (high specificity)
    - Mid-level detect rate (lower than 75% sensitivity)
  - TTP allows for an approximate 10-time increase in the odds of detecting an adversary if the adversary is present
  - Results show that the more information provided to the user, the more successful the operator will be in using the TTP to detect an adversary
- Mitigate: Results show that the more complex the mitigate task, the harder the mitigation becomes
- Recover: TTP was successful in enabling Operators to restore devices to FMC and reintegrate those devices back into network

Defensible Position

There is a reason this soldier is running…

and this one is not…

The owner of this network should be running



Questions?