U.S. ARMY CYBER COMMAND

Operational Technology Cybersecurity

Major Matthew G. Sherburne, P.E.

17 JULY 23

Overall classification of this brief is
UNCLASSIFIED

OPERATE, DEFEND, ATTACK, INFLUENCE, INFORM!

Agenda

1) Purpose
2) About Me
3) Terminology
4) Past OT cybersecurity events
5) Purdue Model
6) MITRE ATT@CK ICS Matrix
7) Federal Level OT Security Documents
8) OT Cybersecurity Documents
9) Industry Specific Guidance
10) Some training programs
11) Q and A

Purpose

- Inform SAME membership about growing focus on OT cybersecurity programs; where to look and how to start.

About Me

- West Point BSEE ’07
- Virginia Tech MSEE ’15
  - Thesis: “Micro Moving Target IPv6 Defense for 6LoWPAN and the Internet of Things”
- Member of IEEE Antennas and Propagation Society and Communications Society
- Amateur Radio Extra Class Operator – KF4WZB
- Licensed Professional Engineer (State of Missouri) since ’19
- Involved in OT cybersecurity since July ’19
  - Former Cyber Protection Team (CPT) Lead – Army OT Focus

Terminology

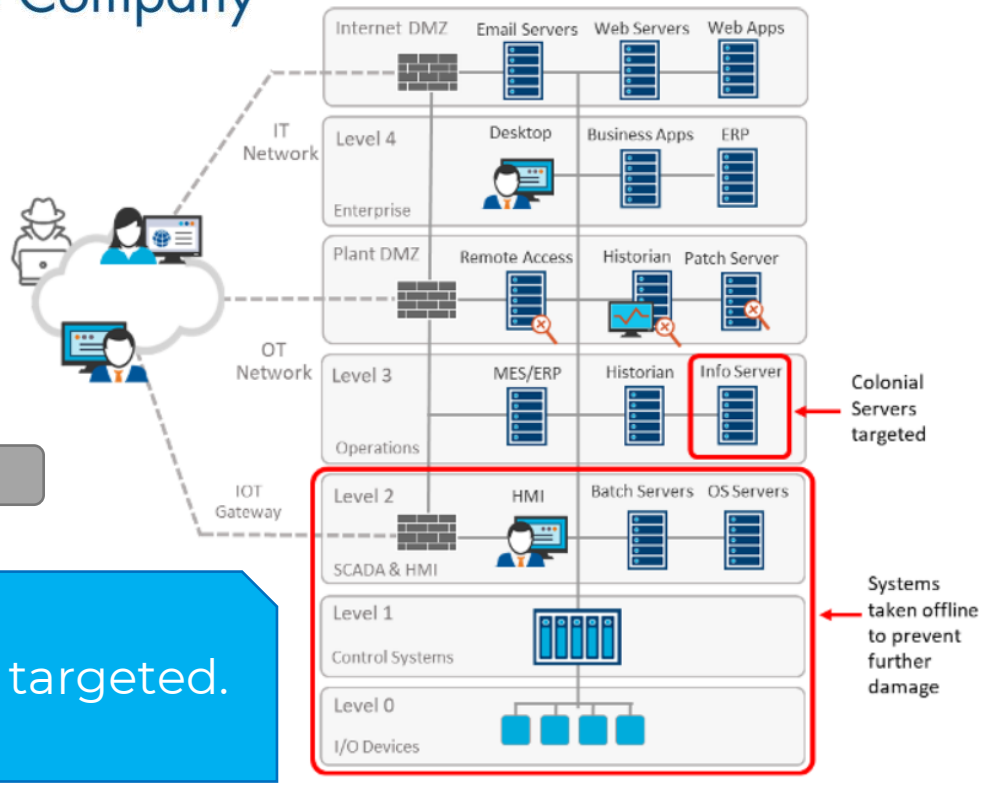
- ICS – Industrial Control Systems
- SCADA – Supervisory Control and Data Acquisition
- FRCS – Facility Related Control Systems
- IACS – Industrial Automation and Control Systems
- SIS – Safety Instrumented System
- OT – Operational Technology (catch-all for ICS/SCADA/FRCS/IACS)
- PLC – Programmable Logic Controller
- RTU – Remote Terminal Unit

Past OT Cybersecurity Events

Date	Target	Method
2000	Australian Sewage Plant	Insider
2010	Iran Uranium Enrichment	Stuxnet
2013	ICS Supply Chain attack	Havex
2014	German Steel Mill	
2015	Ukraine Power Grid	BlackEnergy, KillDisk
2016	Ukraine Substation	CrashOverride
2017	Global shipping company	NotPetya
2017	IoT DDos attack	BrickerBot
2017	Health care, Automotive, many others	WannaCry
2017	Saudi Arabia Petrochemical	TRITON/TRISIS
2019	Norwegian Aluminum Company	LockerGaga

Source: www.awa.csis.org/programs/technology-policy-program/significant-cyber-incidents

Colonial Pipeline Company



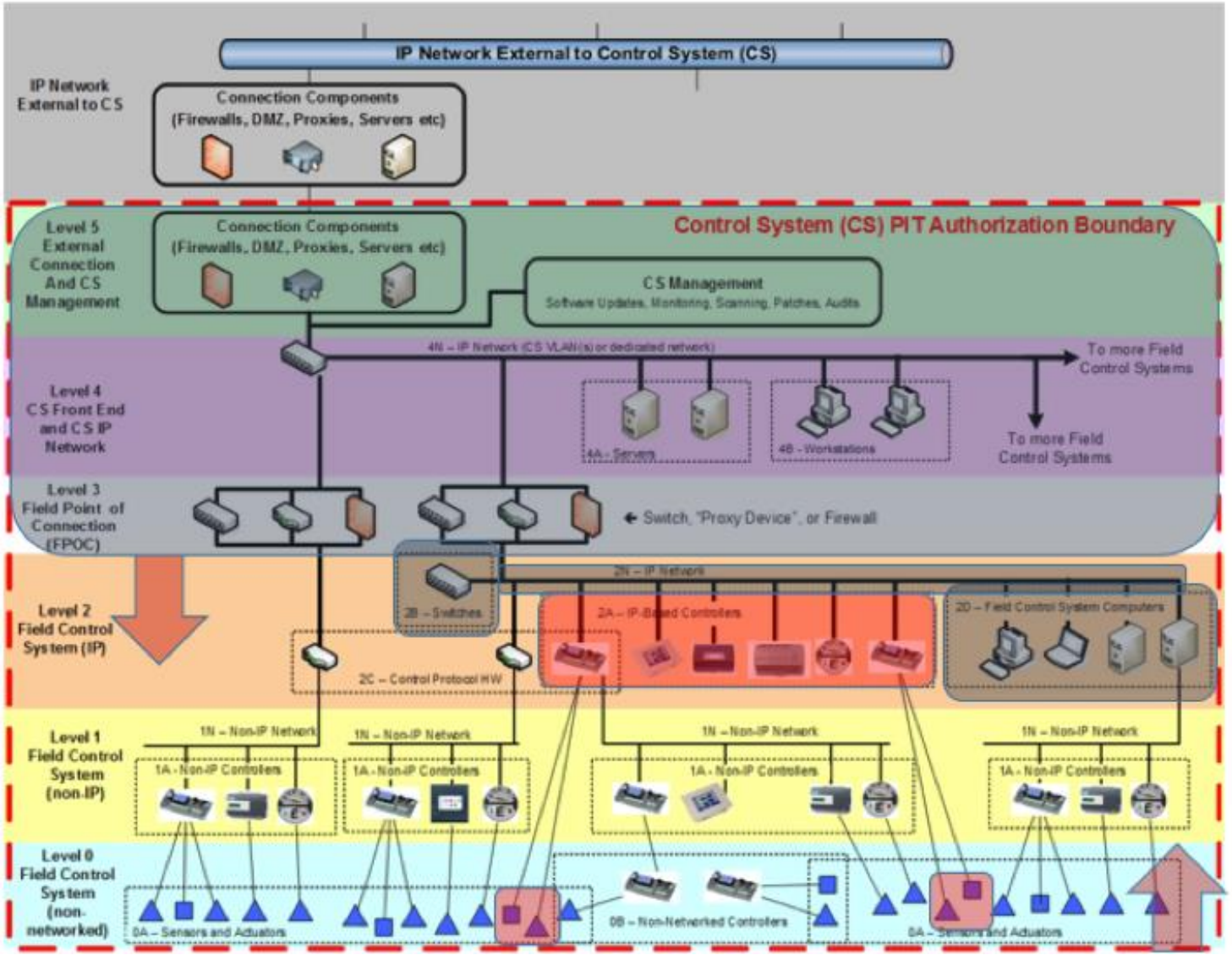
May 2021 Colonial Pipeline →

IT Exploitation can lead to OT disruption, even if not directly targeted.

Figure Source: https://industrial-software.com/community/news/virsec-analysis-of-the-colonial-pipeline-attack/

Table 1: Some notable cyberattacks impacting IACS, https://gca.isa.org/hubfs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf

Purdue Model



"Standard IT" = 50% - 58%

Future IT / OT Convergence

https://www.sans.org/blog/the-risks-of-an-it-versus-ot-paradigm/

MITRE ATT@CK ICS Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	*9 techniques*	*6 techniques*	*2 techniques*	*6 techniques*	*5 techniques*	*7 techniques*	*10 techniques*	*3 techniques*	*13 techniques*	*5 techniques*	*12 techniques*
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Detect Operating Mode		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	I/O Image		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

as of 06MAY22

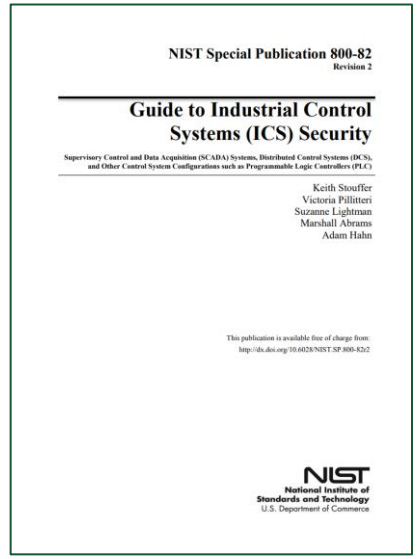
https://attack.mitre.org/matrices/ics/

Federal Level OT Security Documents

- **Homeland Security Presidential Directive 7, 17DEC03**
  - https://www.cisa.gov/news-events/directives/homeland-security-presidential-directive-7
  - "This directive establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks."
- **Executive Order 13636 – Improving Critical Infrastructure Cybersecurity, 12FEB13**
  - https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
- **Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, 12FEB13**
  - https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil/
  - Identifies 16 critical infrastructure sectors
- **Executive Order 13800 – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, 11MAY17**
  - https://www.cisa.gov/topics/cybersecurity-best-practices/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure
- **DHS CISA Cybersecurity Incident and Vulnerability Response Playbooks, Nov '21**
  - https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf
- **NSA,CISA: How Cyber Actors Compromise OT/ICS and How to Defend Against It, Press Release – 22SEP2022**
  - https://media.defense.gov/2022/Sep/22/2003083007/-1/-1/0/CSA_ICS_Know_the_Opponent_.PDF

OT Cybersecurity Documents

- **NIST 800-82, Rev 3 (draft) – Guide to Operational Technology (OT) Security**
  - https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/draft
- **NIST Cybersecurity Framework, FEB14**
  - https://www.nist.gov/cyberframework
  - Identify, Protect, Detect, Respond, Recover
- **ISA99.02.01/IEC 62443: Security for Industrial Automation and Control Systems, JUN20**
  - https://gca.isa.org/hubfs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf


NIST Special Publication 800-82
Revision 2

Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC)

Keith Stouffer
Victoria Pillitteri
Suzanne Lightman
Marshall Abrams
Adam Hahn

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-82r2

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Industry Specific Guidance

- North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP)
  - https://www.nerc.com/pa/Stand/Pages/USRelStand.aspx

- Transport Security Administration (TSA) Pipeline Security Guidelines, April 21
  - https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf

Training your Workforce (a way)

DHS CISA Virtual Training

- https://www.cisa.gov/ics-training-available-through-cisa

In-person training at Idaho Falls, Idaho

- Industrial Control Systems Cybersecurity 301L (next 4 day course May 15-18)
- Industrial Control Systems Evaluation 401L (next 3 day course May 23-25)
- https://www.cisa.gov/ics-training-calendar

SANS Institute Training

- **https://www.sans.org/cyber-security-courses/?focus-area=industrial-control-systems-security**

- **SANS ICS410: ICS/SCADA Security Essentials**
  - Associated Cert: GIAC Global Industrial Cyber Security Professional
- **SANS ICS515: ICS Visibility, Detection, and Response**
  - Associated Cert: GIAC Response and Industrial Defense
- **SANS ICS612: ICS Cybersecurity In-Depth**

- **SANS ICS456: Essentials for NERC Critical Infrastructure Protection**
  - Associated Cert: GIAC Critical Infrastructure Protection
- **SANS ICS418: ICS Security Essentials for Managers**

NDAA 22 § 1505 Awareness

(f) SERVICE RESPONSIBILITIES. [*abridged*]

(1) ensure that relevant local network and cybersecurity forces are responsible for defending
operational technology

(2) ensure that relevant local operational technology- focused system operators, network and
cybersecurity forces, mission defense teams and other service-retained forces, and cyber protection teams are appropriately trained,

(3) ensure that all Defense Critical Assets and Task Critical Assets are monitored and defended by Cybersecurity Service Providers,

(4) ensure that operational technology is appropriately sensored and appropriate cybersecurity defenses,

(5) implement Department of Defense Chief Information Officer policy germane to operational technology

(6) plan for, designate, and train dedicated forces to be utilized in operational technology-centric roles across the military services and United States Cyber Command,

(7) ensure that operational technology, as appropriate, is not easily accessible via the internet
and that cybersecurity investments accord with mission risk to and relevant access vectors for Defense Critical Assets and Task Critical Assets.

SEC. 1505. OPERATIONAL TECHNOLOGY AND MISSION-RELEVANT TERRAIN IN CYBERSPACE.

(a) MISSION-RELEVANT TERRAIN.—Not later than January 1, 2025, the Secretary of Defense shall complete mapping of mission-relevant terrain in cyberspace for Defense Critical Assets and Task Critical Assets at sufficient granularity to enable mission thread analysis and situational awareness, including required—

(1) decomposition of missions reliant on such Assets;
(2) identification of access vectors;
(3) internal and external dependencies;
(4) topology of networks and network segments;
(5) cybersecurity defenses across information and operational technology on such Assets; and
(6) identification of associated or reliant weapon systems.

(b) COMBATANT COMMAND RESPONSIBILITIES.—Not later than January 1, 2024, the Commanders of United States European Command, United States Indo-Pacific Command, United States Northern Command, United States Strategic Command, United

14 JUN 23 – AUSA Hot Topic

Panel on OT Cybersecurity moderated by the Army's Principal Cyber Advisor –Dr. Sulmeyer.

To watch visit AUSA

The cybersecurity of Operational Technology and Critical Resources is a major focus area for the Army.

QUESTIONS & CLOSING
COMMENTS

BACKUP SLIDES

Date	Target	Method	Significance
2000	Australian Sewage Plant	Insider	Release of 265,000 gallons of untreated sewage into local parks and rivers
2010	Iran Uranium Enrichment	Stuxnet	1st reported cyber attack to cause physical damage
2013	ICS Supply Chain attack	Havex	Wide-spread ICS reconnaissance – 1st identified malware specifically geared to look at common ICS TCP port traffic
2014	German Steel Mill		2nd Cyber attack to cause physical damage and confirmed by a legitimate government source
2015	Ukraine Power Grid	BlackEnergy 3	Loss of power to 230,000 customers for 6 hours. (30 substations taken offline)
2016	Ukraine Substation	Industroyer	Automated attack that hit a single transmission substation in northern Kiev
2017	Global shipping company	NotPetya	$300 million loss and global delays for Maersk
2017	IoT DDoS Attack	BrickerBot	Reportedly destroyed 10 million IoT devices and influenced the Silex malware two years later
2017	Health care, Automative, many others	WannaCry	Began 12May2017 and stopped shortly after discovery of a kill switch. Mass impact.
2017	Saudi Arabia Petrochemical	TRITON/TRISIS	Specifically engineered to disable safety instrumented systems like Triconex.
2019	Norwegian Aluminum Company	LockerGoga	Norsk Hydro impacted by ransomware delivered by phishing attack.
2021	US Oil Pipeline Company		The largest publicly disclosed cyber attack against critical infrastructure in the US. Colonial Pipeline attacked by ransomware. Impacted IT based billing systems. Did not touch OT. Exposed VPN password led to delivery of ransomware by the DarkSide group on 06MAY21. Pipeline restarted on 12MAY21. Separately employee reused a password that also was potentially exploited.