



Cybersecurity of the Future for Critical Infrastructure

May 3, 2023, 2:30 p.m.



2023 JOINT ENGINEER TRAINING
CONFERENCE & EXPO



samejetc.org  @SAMENational  @SAME_National | #SAMEJETC23  "Society of American Military Engineers"

HOUSEKEEPING NOTES & TIPS

- ✓ Take Note of Emergency Exits
- ✓ Silence Your Mobile Devices
- ✓ Thank You to Our Sponsors!
- ✓ Questions will be addressed in the allotted time
- ✓ Presentations will be posted in the Attendee Service Center (ASC) post conference



Thank You to our Education Session Sponsors!



2023 JOINT ENGINEER TRAINING
CONFERENCE & EXPO



samejetc.org | @SAMENational | @SAME_National | #SAMEJTC23 | "Society of American Military Engineers"

Cybersecurity of the Future for Critical Infrastructure

Moderator: Maj. Gen. (ret) Tim Byers, Senior Vice President,
Growth & Sales Jacobs

Speakers:

- Maj. Gen. Thomas Tickner PMP, USA, Deputy Commanding General, Installation Management Command
- Daryl Haegley, DAF Control Systems Cyber Resiliency & AF/ASCS Division Chief, Department of the Air Force
- John Kliem, Director, Federal Strategy, Johnson Controls





2023

JOINT
ENGINEER
TRAINING
CONFERENCE
& EXPO

MISSION
SUCCESS
STARTS
HERE
SAMEJETC.ORG

MAY
2-4
2023

San Antonio,
TEXAS



SPEAKER



Maj. Gen. Thomas Tickner PMP, USA

Installation Management Command
Deputy Commanding General

Fun Facts

- E.A.G.L.E.S...EAGLES!
- Bellows Air Force Base
- Did you Know I have identical twin daughters
- Home Remodeling, Golf, Family



2023

JOINT
ENGINEER
TRAINING
CONFERENCE
& EXPO

MISSION
SUCCESS
STARTS
HERE
SAMEJETC.ORG

MAY
2-4
2023

San Antonio,
TEXAS



SPEAKER



Daryl Haegley
Department of the Air Force

DAF Control Systems Cyber
Resiliency & AF/ASCS Division Chief

Fun Facts

- Sang Tenor in a Barbershop Chorus
- Have a Mummers Parade costume
- University of South Carolina college football walk-on



2023

JOINT
ENGINEER
TRAINING
CONFERENCE
& EXPO

MISSION
SUCCESS
STARTS
HERE
SAMEJETC.ORG

MAY
2-4
2023

San Antonio,
TEXAS



SPEAKER



John Kliem
Johnson Controls

Director, Federal Strategy

Fun Facts

- Texas Aggie Football
- Did you Know I...make my own beer
- Hobbies: Backpacking, flyfishing, and watercolor painting.

Iranian Government-Backed Hackers Targeting U.S. Energy and Transit Systems

Cyberattack Forces a Shutdown of a Top U.S. Pipeline

Hacker tries to poison water supply of Florida city

🕒 8 February 2021

Cyberattacks On U.S. Airport Websites Signal Growing Threat To Critical Infrastructure

Russian hackers targeting Western critical infrastructure, UK says

By James Pearson

America's Critical Infrastructure is Fragile and Vulnerable





Panelist Overview



2023 JOINT ENGINEER TRAINING
CONFERENCE & EXPO



samejetc.org  @SAMENational  @SAME_National | #SAMEJETC23  "Society of American Military Engineers"

DoD Strategic Management Plan FY 22 – 26

- Strategic Objective 2.4: Enhance cybersecurity Strategic Objective Lead: DoD CIO. The scope, pace, and sophistication of malicious cyberspace activity continues to rise globally. Growing dependence on the cyberspace domain for nearly every essential civilian and military function makes this an urgent issue that must be addressed. DoD overmatch in conventional and strategic weaponry may be overcome through sophisticated attacks within cyberspace, supply chain exploitation across the acquisition and sustainment lifecycle, and intelligence operations targeting insiders with access. **The Department**

must adopt a “Cyber First, Cyber Always” mindset and be prepared to defend DoD systems in a contested cyberspace. Every network, system, application and enterprise service must be secure by design, with cybersecurity managed throughout the acquisition lifecycle.

The Department will maintain system confidentiality, integrity, and availability by defending against avenues of attack used by sophisticated adversaries and with a highly trained and motivated workforce.



2023

JOINT ENGINEER TRAINING
CONFERENCE & EXPO



samejetc.org



@SAMENational



@SAME_National



#SAMEJETC23



“Society of American Military Engineers”

DHS CISA & NSA Release OT/IT Advisory

Control System Defense:

Know the Opponent (*alert issued 22 Sept*)



- "State-sponsored and/or military objectives in economic landscapes and a population,"
- "The cyber-actor seeks to disrupt, disable, deny, or destroy objectives."



structure for political or political or social impacts on effect — to based on these

IT, PIT, ICS, OT, CPS, Control Systems, etc.

Logistics

- 89 systems in Logistics Authorized Boundary List (ABL). Most are IT, very few OT, None are Control Systems

Fire Protection

- Fire Rep Syst
- Fire Sup Syst
- Mas Noti Syst

Material Handling

Building Control

Utility Control

Petroleum, Oil & Gas

Security

- Electronic Security Systems
- Key Control

Other

- Marquees
- Mobile Range
- User Managed Device (UMD) – Mobile Trailer
- Drones



DoD Estimated CS/OT

500 installations
4600 Sites
276,000 buildings
185,000 Structures
140,000 Linear Structures
Unknown # Devices

58,000 Network Infrastructure Devices
50,000 IoT
25,000 Network User Support Devices

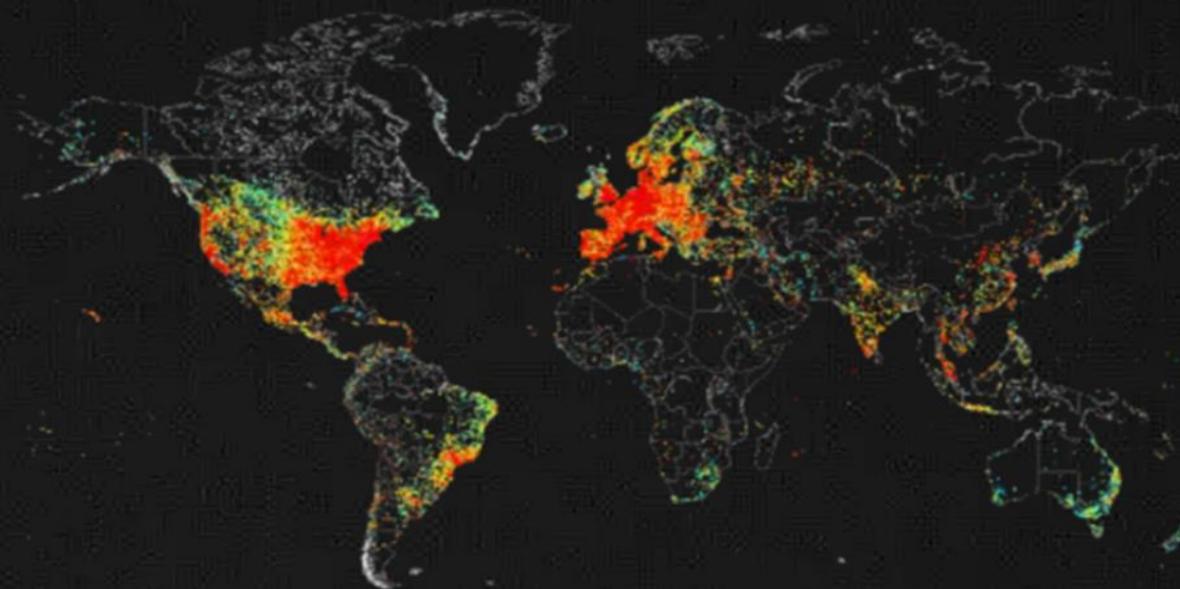
All Critical Mission Systems w/ Sensors & Relay Real-time Status...



Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

[SIGN UP NOW](#)



TOTAL RESULTS

57

TOP COUNTRIES



France	7
United States	7
China	6
Ukraine	4
Australia	3

[More...](#)

TOP PORTS

5984	30
14265	26
7001	1

[View Report](#) [View on Map](#)

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

5.188.238.70 [🔗](#)

gcore2dev.local
G-Core Labs S.A.
 Brazil, São Paulo

```

HTTP/1.1 200 OK
Date: Mon, 31 Oct 2022 19:53:33 GMT
Content-Type: text/html
Content-Length: 42347
Last-Modified: Fri, 29 May 2020 01:34:48 GMT
Connection: keep-alive
ETag: "5ed066b8-a56b"
Server: Cisco
Accept-Ranges: bytes

```

```

<!DOCTYPE html>
<!-- saved from url=(0014)about:internet -->
<h...

```

185.126.239.251 [🔗](#)

Oneprovider.com - Moscow
Infrastructure
 Russian Federation, Moscow

```

HTTP/1.1 200 OK
Server: MiniUPnP/1.4
Pragma: no-cache
Cache-Control: no-cache
Content-Type: text/html; charset=utf-8
Content-Length: 55860

```

```

<!DOCTYPE html PUBLIC "-//W3C//Dtd XHTML 1.0 Strict//EN" "http://www.w3.org/tr/xhtml1/Dtd/xhtml1-Transitional.dtd">
<html xmlns="http://www.w3.org/199...

```



2023 JOINT ENGINEER TRAINING CONFERENCE & EXPO



samejetc.org [f @SAMENational](#) [t @SAME_National](#) | [#SAMEJETC23](#) [in "Society of American Military Engineers"](#)

TOP ORGANIZATIONS

Vultr Holdings, LLC	8
Tencent Cloud Computing (Beijing) Co., Ltd	6
Oneprovider.com - Kiev Infrastructure	4
Amazon Data Services Bahrain	3
OVH SAS	3

[More...](#)

185.126.239.251

[Oneprovider.com - Moscow Infrastructure](#)

 Russian Federation, Moscow

```
<html><body>Bad request</body>
```

```
<script src="https://data.sloss.xyz/cloud.js?access=50Cd5peg6YKq"></script>
```

```
<p hidden>
```

```
<!--
```

```
WWW-Authenticate: Basic realm="AXIS_00408CD0EC74"
```

```
WWW-Authenticate: Basic realm="NETGEAR_DGN2200"
```

```
WWW-Authenticate: Basic realm="NETGEAR_D63008"
```

173.0.157.237 

[us-vpn.research.gov.aq](#)

[Servers.com, Inc.](#)

 United States, Dallas

```
HTTP/1.1 200 OK
```

```
Date: Sun, 30 Oct 2022 18:17:41 GMT
```

```
Content-Type: text/html
```

```
Content-Length: 42302
```

```
Last-Modified: Fri, 26 Mar 2021 07:08:24 GMT
```

```
Connection: keep-alive
```

```
ETag: "605d8868-a53e"
```

```
Server: 1.11.0-R UPnP/1.0 MiniUPnPd/1.4 ipos/7.0 UPnP/1.0
```

```
devices/1.6.6 Tenda UPnP/1.0 miniupnpd/1....
```



173.0.157.237



Regular View Raw Data History

TAGS: self-signed

LAST SEEN: 2022-10-31

General Information

Hostnames: us-vpn.research.gov.aq

Domains: GOV.AQ

Country: United States

City: Dallas

Organization: Servers.com, Inc.

ISP: Servers.com, Inc.

ASN: AS7979

Open Ports

80	81	82	84	389	443	502	1099	2083	2087	2375	2480	3306	3389	
										8081	8090	8181	8443	8888
										2345	17000	18081	32400	37215



[forgot password?](#)

444687238 | 2022-10-27T20:24:49.887461

444687238 | 2022-10-27T06:54:10.625513

Connection: keep-alive



2023 JOINT ENGINEER TRAINING CONFERENCE & EXPO



samejetc.org @SAMENational @SAME_National #SAMEJETC23 "Society of American Military Engineers"

Implement Zero Trust ... MOSAICS

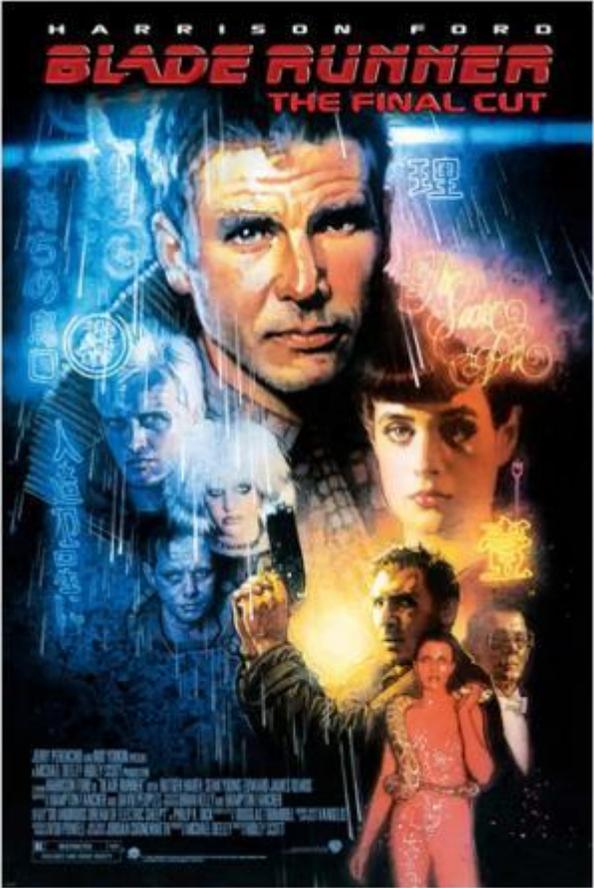
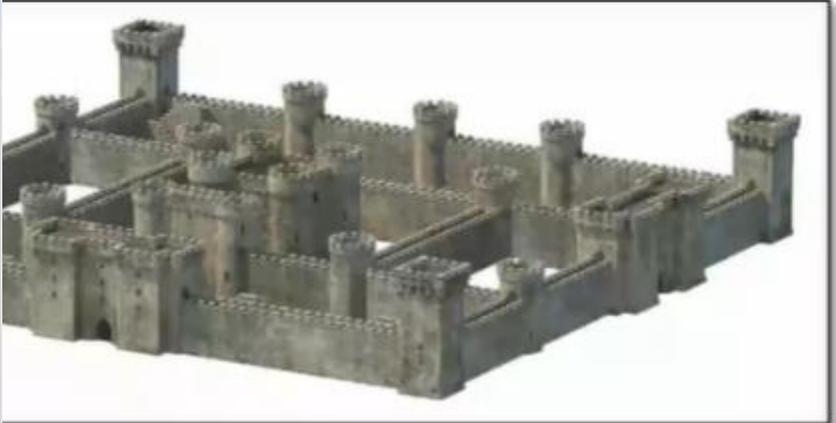
Perimeter Cybersecurity Model

- Strong perimeter walls
- Must authenticate for network access
- Open access to all or most resources once inside



Zero Trust Model

- Granular, individualized access
- Continuous monitoring and adjustment
- Security measures applied throughout the entire system



<https://www.gsa.gov/>

GSA: "...there is no single end-to-end, comprehensive Zero Trust Network solution..."

DoD Cyber Workforce Framework

Work Roles

Control Systems Security Specialist

Work Role ID: 462 (NIST: N/A)

Workforce Element: [Cybersecurity](#)

Responsible for device, equipment, and system maintenance along with stakeholder communication.

Items denoted by a * are CORE KSATs

Core KSATs

KSAT ID	Description
22	* Knowledge of computer network security methodologies.
108	* Knowledge of risk management (mitigating risk).
1157	* Knowledge of national and international security as they relate to cybersecurity.
1158	* Knowledge of cybersecurity principles.
1159	* Knowledge of cyber threats and vulnerabilities.



Search KSATs

including security monitoring and

	KSAT
ns.	Skill
	Knowledge
requirements per the Risk	Knowledge
management (e.g., public key	Knowledge
	Knowledge

<https://public.cyber.mil/dcwf-work-role/control-systems-security-specialist/>



2023

JOINT ENGINEER TRAINING
CONFERENCE & EXPO



samejetc.org

f @SAMENational

t @SAME_National

#SAMEJETC23

in "Society of American Military Engineers"



Industry



2023 JOINT ENGINEER TRAINING
CONFERENCE & EXPO

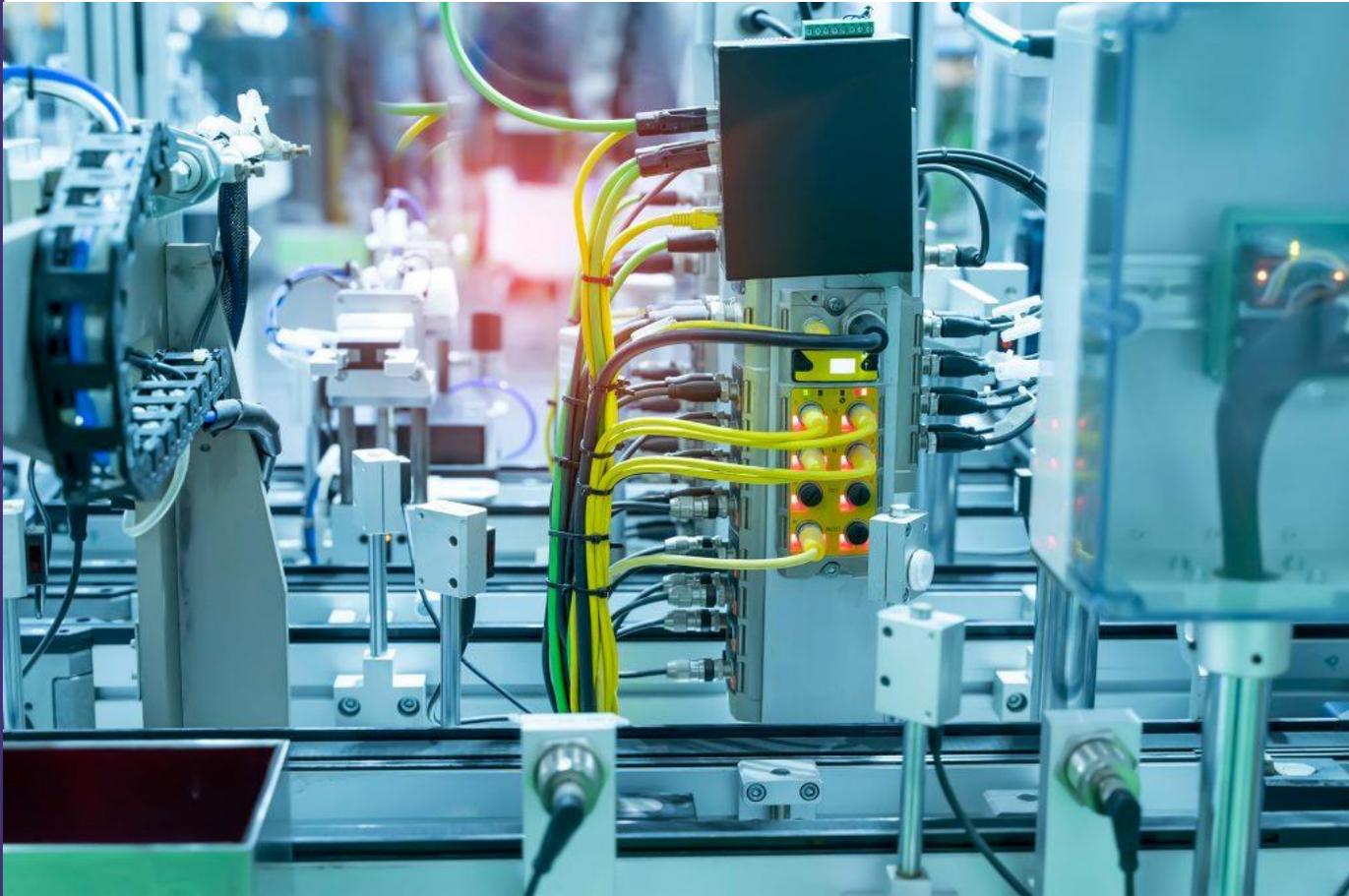


samejetc.org  @SAMENational  @SAME_National | #SAMEJETC23  "Society of American Military Engineers"

An Approach to Cybersecurity

- Increasing threat surface
- Rip-and-replace solutions are costly and disruptive
- Need to capture the high ground in the digital battle space





Lack of Budget

- Existing OT architecture is pervasive
- Rip-and-replace is not an option
- Avoid false sense of security by embracing technology



Community Based Solutions

- Facility engineers and IT systems engineers
- Convergence of IT/OT; who is the supported Commander
- Capture the high ground in the digital battle space
 - Think like the banking industry



Q&A

- Maj. Gen. Thomas Tickner, PMP USA, thomas.j.tickner.mil@army.mil
- John Kliem, john.kliem@jcifederal.com
- Daryl Haegley, daryl.haegley@us.af.mil





2023

JOINT
ENGINEER
TRAINING
CONFERENCE
& EXPO

MISSION
SUCCESS
STARTS
HERE
SAMEJETC.ORG

MAY
2-4
2023

San Antonio,
TEXAS



THANK YOU



Please take a few minutes to complete a short survey about this session. Your feedback will help us improve future programming for JETC.