The Risk & Reward Of Distributed Industrial Control

Joe Slowik, Principal Intelligence Analyst & ATT&CK CTI Lead

@jfslowik

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Intros

- Joe Slowik
  - MITRE ATT&CK CTI Lead, Critical Infrastructure Security
  - Previous:
    - Various Roles In CTI, DE&TH
    - CTI Training & Teaching

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

Agenda

- Distributed Industrial Operations
- Extending The Attack Surface
- Adversary Opportunities
- Risks & Considerations

MITRE

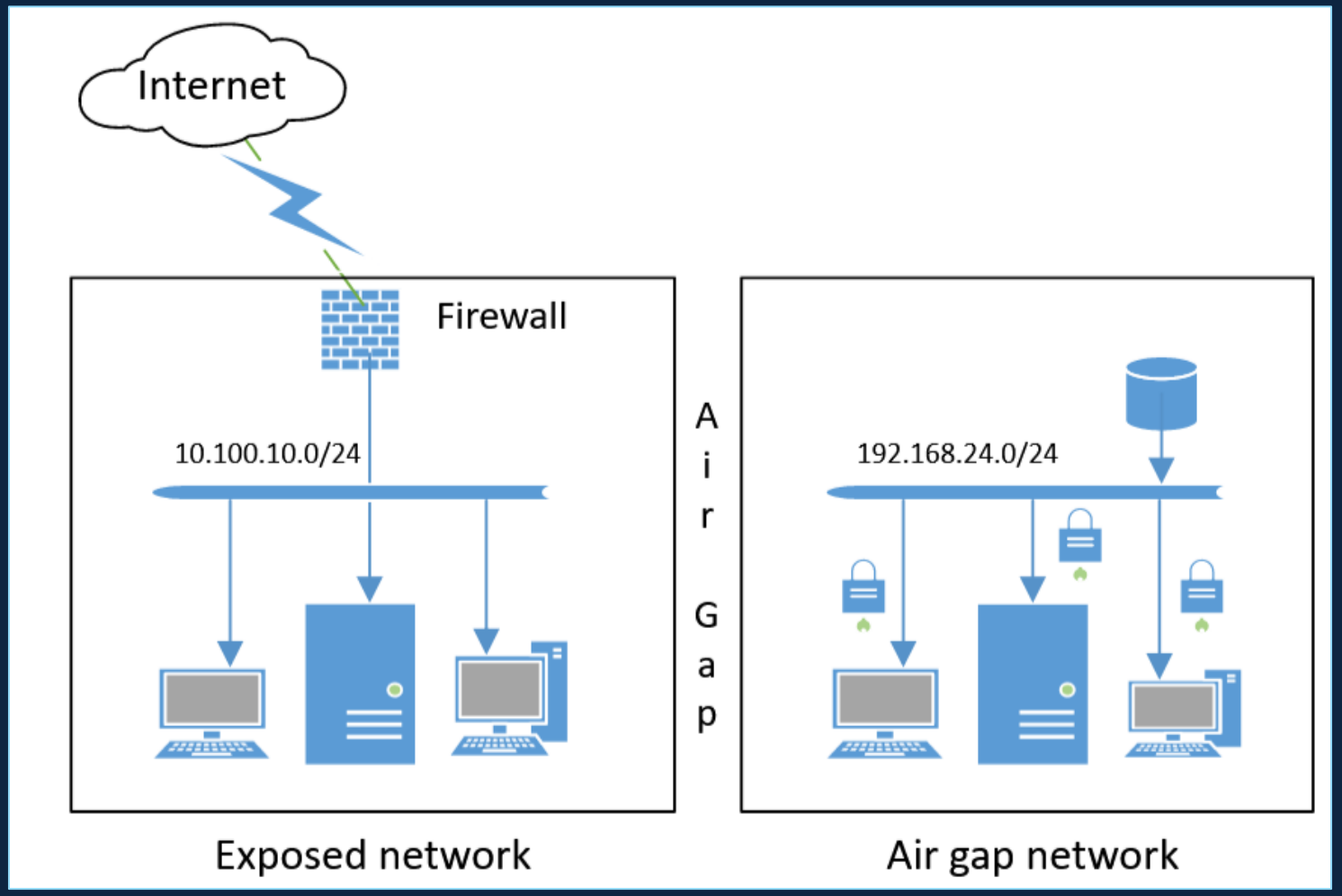
© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

Distributed Industrial Operations

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

OT Network Popular Perception

Distributed Industrial Operations



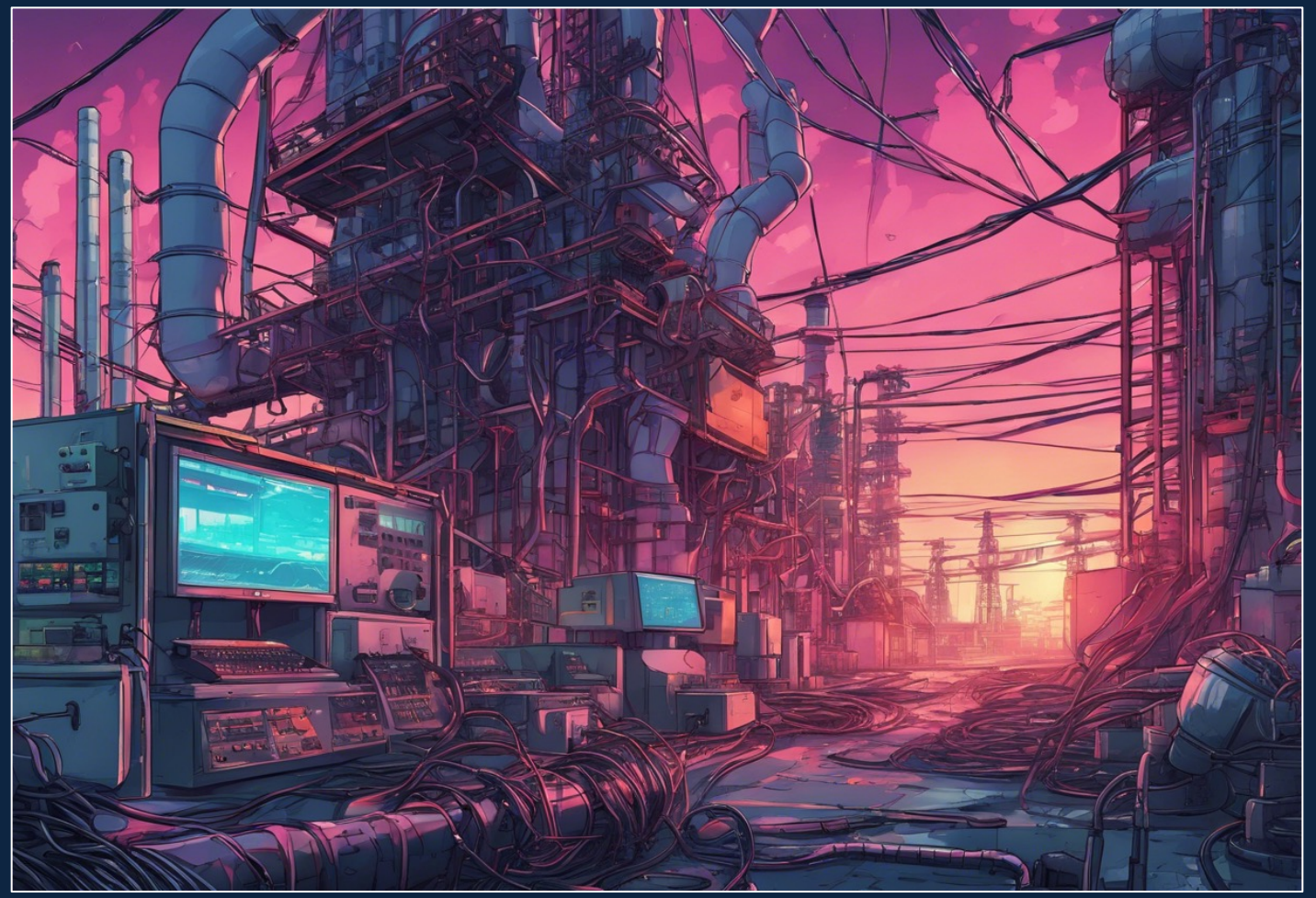
https://upload.wikimedia.org/wikipedia/commons/d/da/Air_gap_network.png

MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

We’re All Living In A Networked World

Distributed Industrial Operations



MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

Embracing The Modern

Distributed Industrial Operations

Legacy Environments

- Operations & Control Co-Located
- Plant Networks Stop At The Facility Boundary

Modern Operations

- Distributed Operations & Lack Of Manning
- Remote Control & Operation Are Necessary

MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

This Isn’t Really New…

Distributed Industrial Operations



https://www.cnet.com/a/img/resize/994bd75863406f3a53c1cc9617aa8c94f27682b2/hub/2010/08/19/3f910eaa-f0fa-11e2-8c7c-d4ae52e62bcc/ISO_New_England_Control_Room_large_jpg.JPG?width=1200

https://i0.wp.com/www.securityguardexam.com/wp-content/uploads/2020/03/security-control-room-1.jpg?fit=560%2C420&ssl=1



MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

But Is HAS Become Far More Prevalent

Distributed Industrial Operations

Economics & Efficiency Have Driven Unmanned, Remote Operations

Technology Advances Permit Easier Connectivity With Remote Assets

Industry Trends Like DERs & Vendor Remote Telemetry Accelerate These Trends

MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

Remote Connectivity Options

Distributed Industrial Operations

POTS

Dedicated Fiber

Cellular Modem

VSATs & Satellite Systems

5G & Wireless Technologies

MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

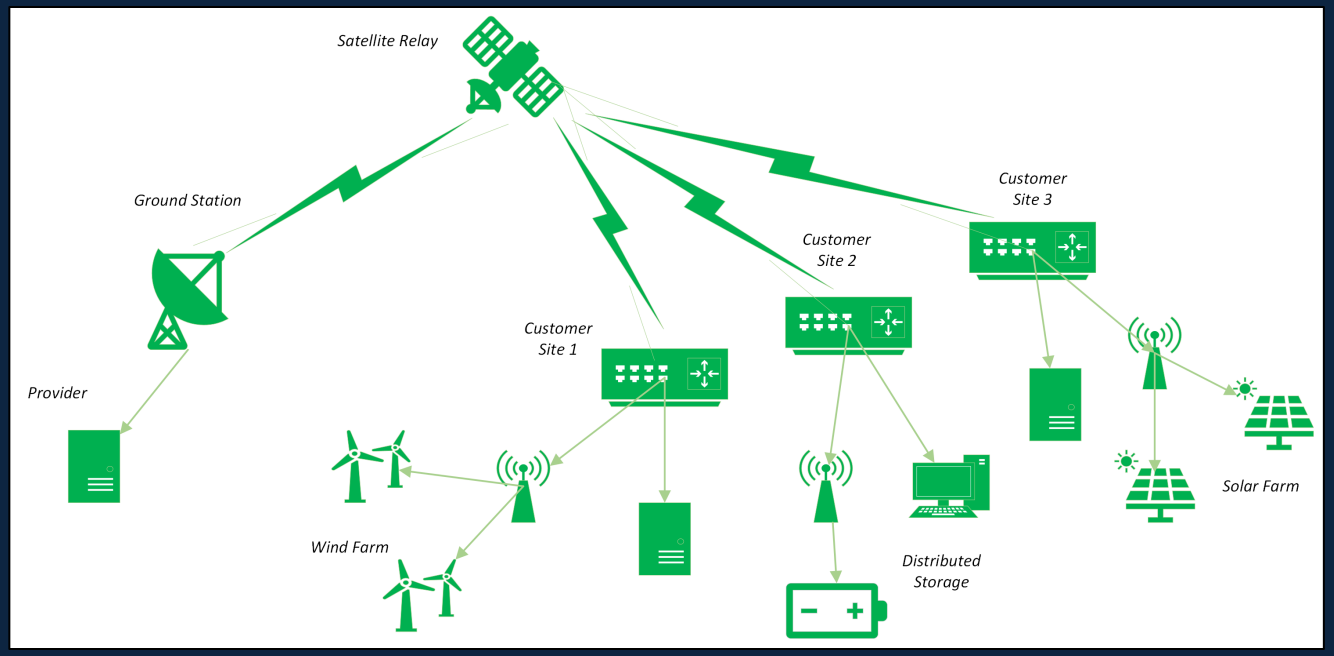
Extending The Attack Surface

MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

Always Online Industrial Systems

Extending The Attack Surface

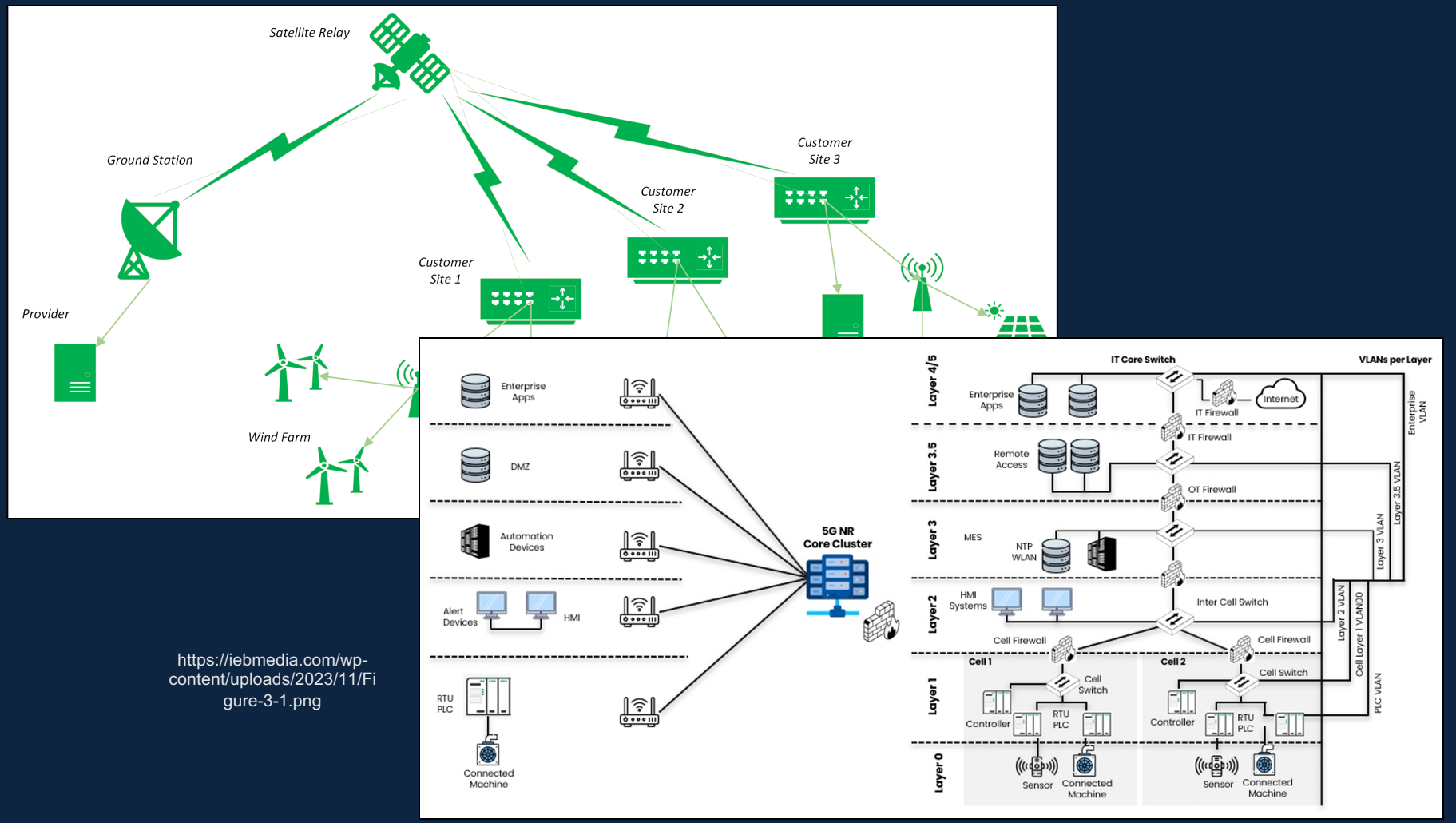


MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

Always Online Industrial Systems

Extending The Attack Surface



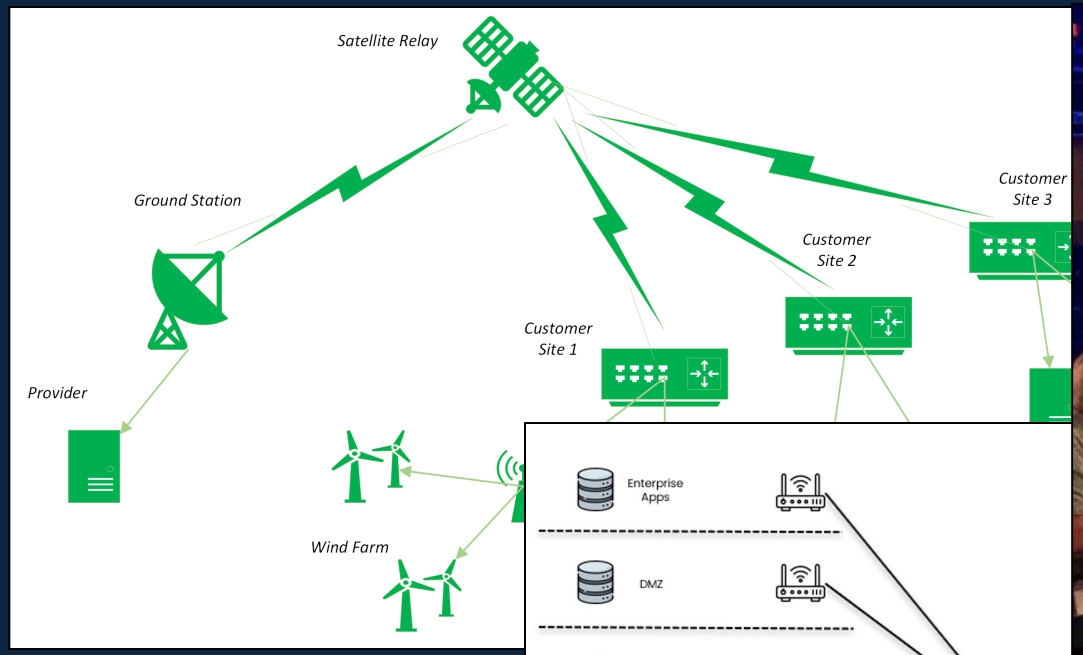
https://iebmedia.com/wp-content/uploads/2023/11/Figure-3-1.png

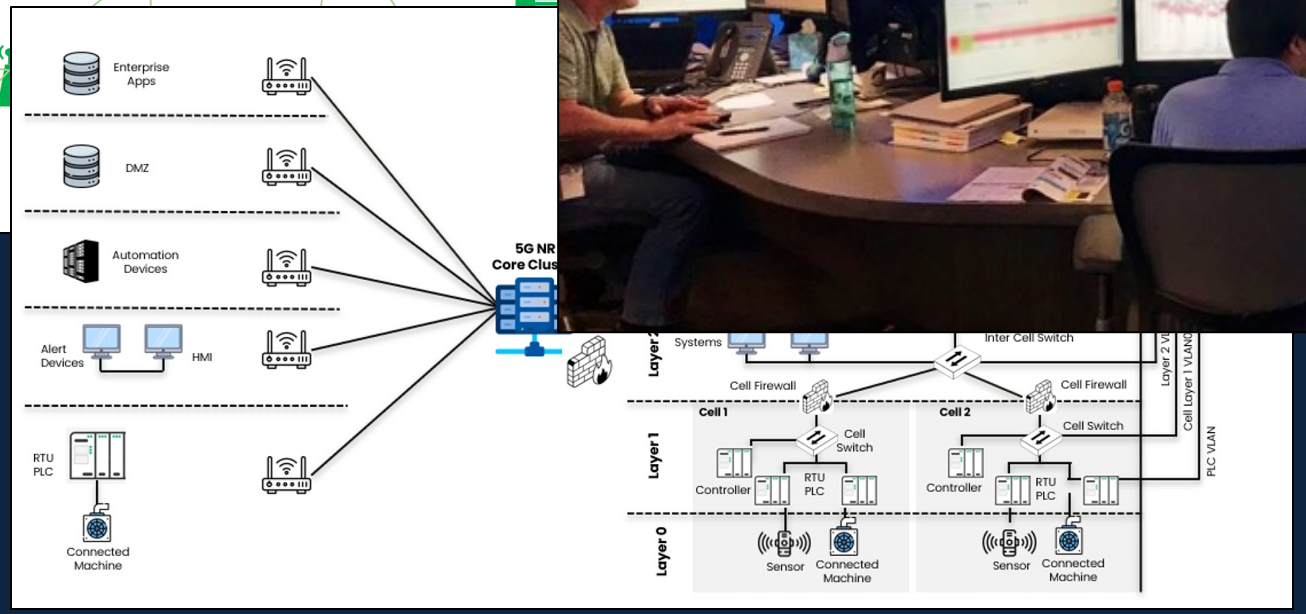
MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

Always Online Industrial Systems

Extending The Attack Surface







https://iebmedia.com/wp-content/uploads/2023/11/Figure-3-1.png

https://www.ge.com/news/sites/default/files/Picture1.png

MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

Connectivity Functions & Dependencies

Extending The Attack Surface

Remote Access & Maintenance

Remote Control & Operations

Telemetry & Health Check

Licensing & Use Monitoring

Coordination, Balancing, & Management

MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

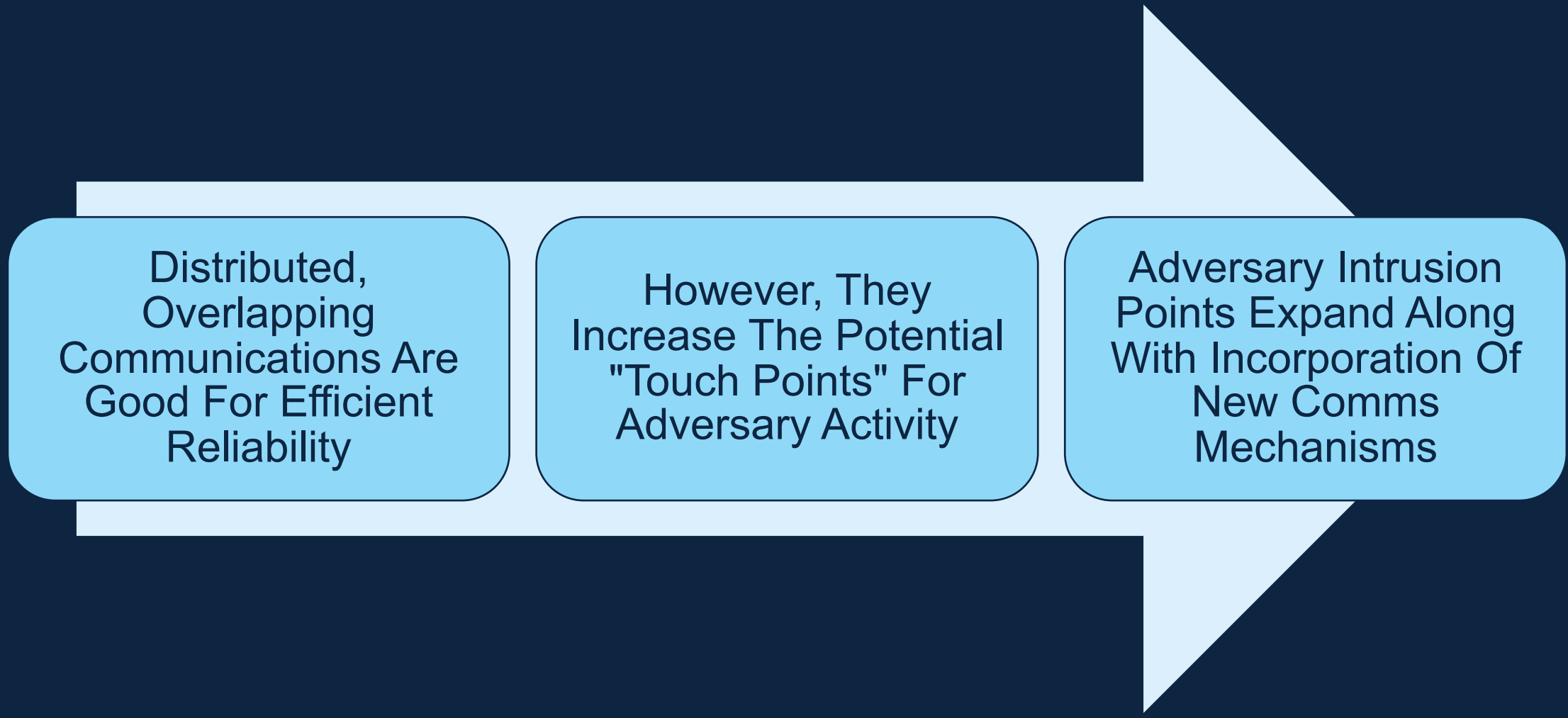
Adversary Opportunities

MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

Extending The Attack Surface

Adversary Opportunities



© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

Enercon & SATCOM Disruption

Adversary Opportunities



https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/

https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

AcidRain | A Modem Wiper Rains Down on Europe

JUAN ANDRÉS GUERRERO-SAADE / MARCH 31, 2022

By Juan Andres Guerrero-Saade (@juanandres_gs) and Max van Amerongen (@maxpl0it)

Executive Summary

- On Thursday, February 24th, 2022, a cyber attack rendered Viasat KA-SAT modems inoperable in Ukraine.
- Spillover from this attack rendered 5,800 Enercon wind turbines in Germany unable to communicate for remote monitoring or control.

MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

The Colonial Pipeline Incident*

Adversary Opportunities

America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home / News & Events / News

BLOG

The Attack on Colonial Pipeline: What W… Learned & What We've Done Over the Pa… Years

Released: May 07, 2023

Jen Easterly, CISA Director

Tom Fanning, Chairman and CEO of Southern Company and Chair of CISA's Cybersecurity Advisory Com…

RELATED TOPICS: ORGANIZATIONS AND CYBER SAFETY, INDUSTRIAL CONTROL SYSTEMS, CRITICAL INFRASTRUCTURE SECURITY …

https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/

Reuters

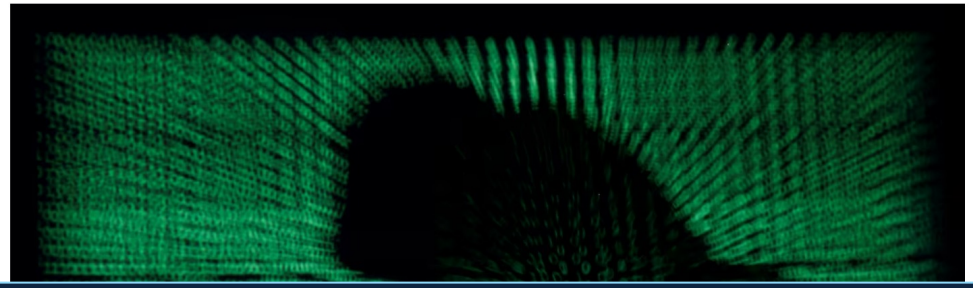
World | Business | Markets | Sustainability | Legal | Breakingviews | Technology | Investigations | More

Technology

Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed

By **Christopher Bing** and **Stephanie Kelly**

May 7, 2021 10:54 PM MDT · Updated 3 years ago

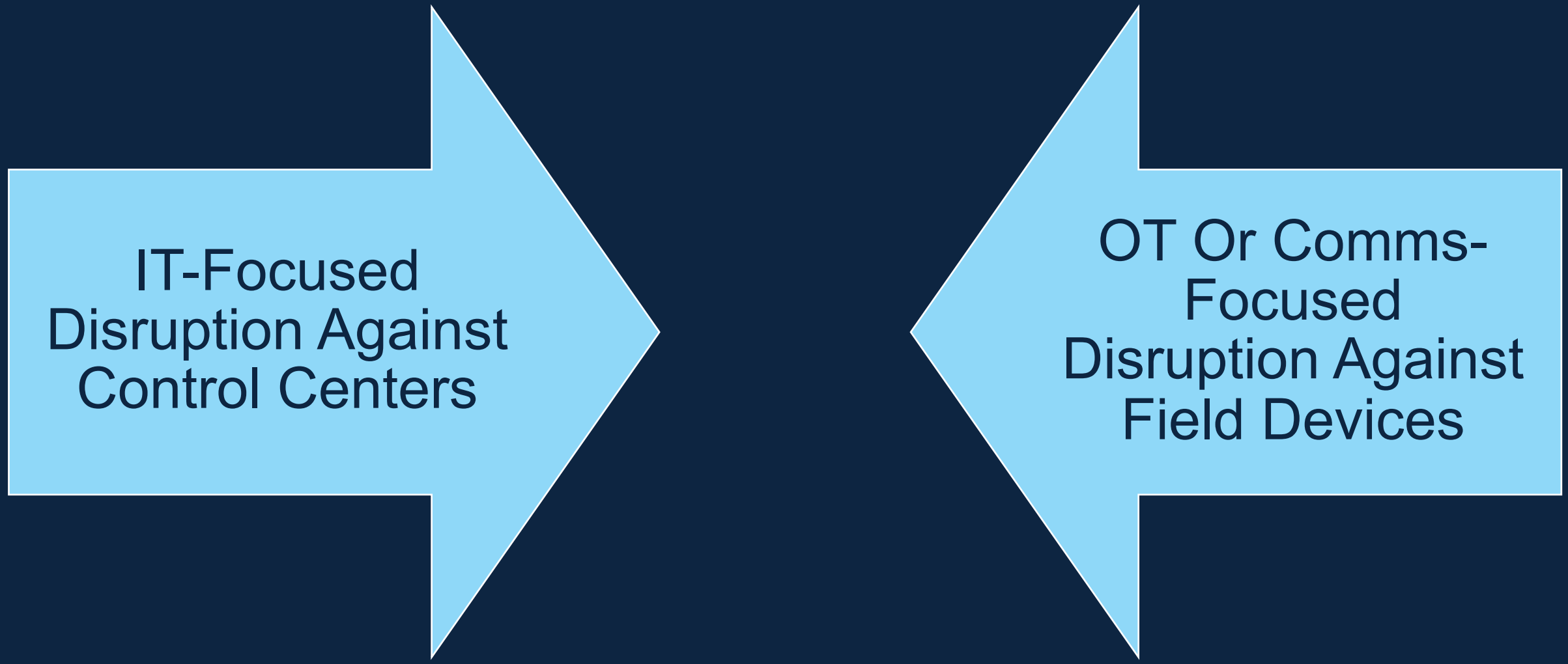


MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

Diverse Opportunities

Adversary Opportunities

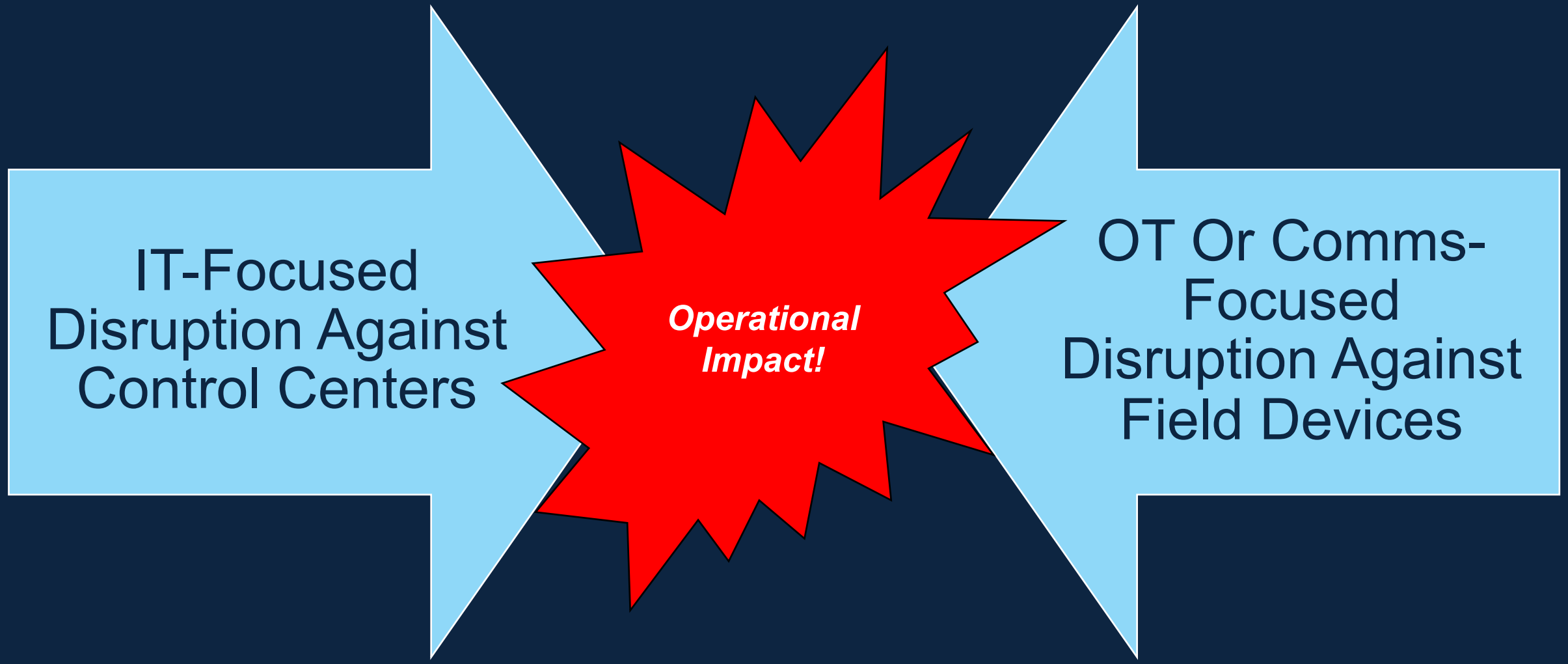


MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

Diverse Opportunities

Adversary Opportunities

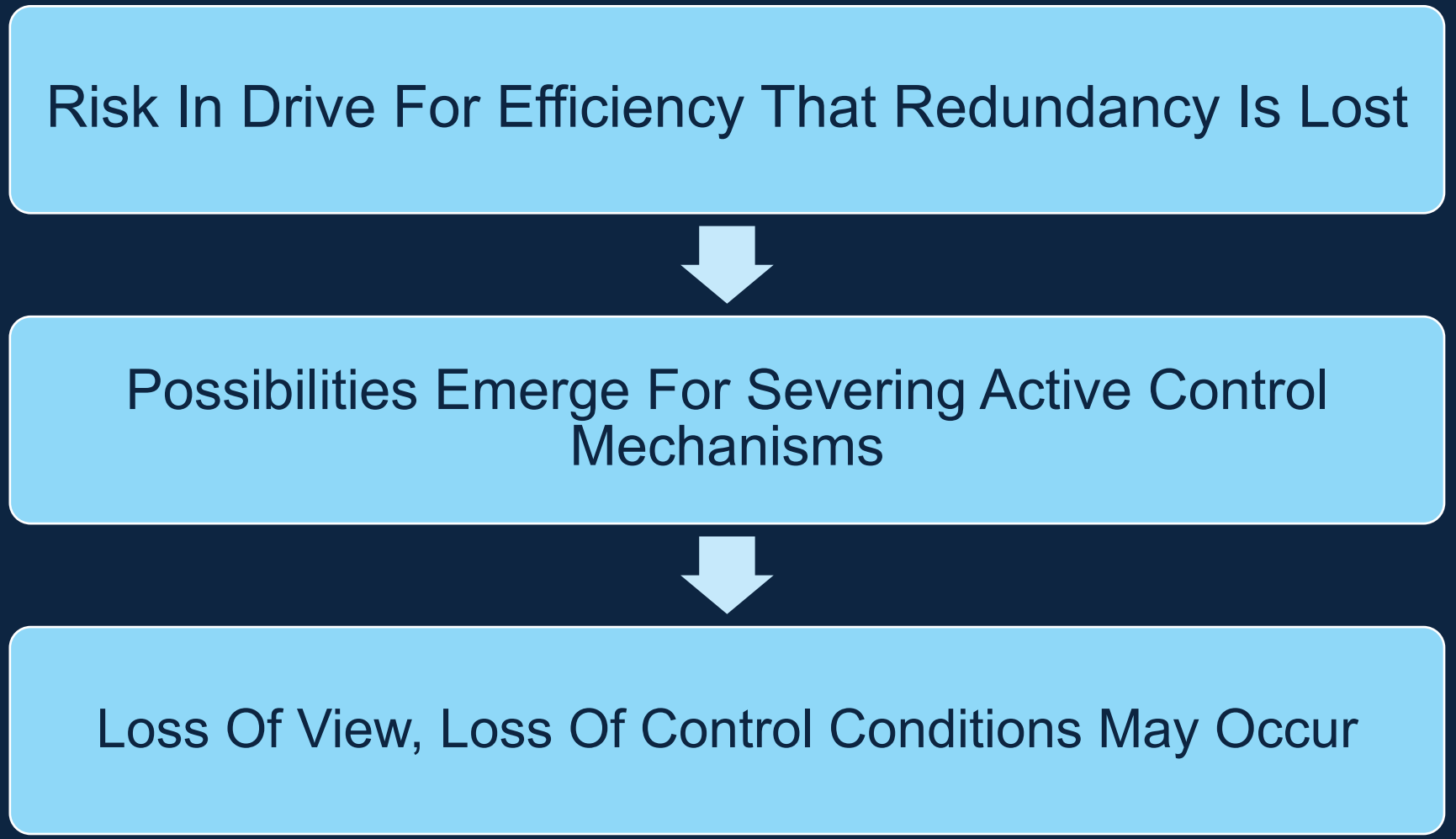


MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

Dependencies & Disruption

Adversary Opportunities



MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

Risks & Considerations

MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

Turn Back The Clock?

Risks & Considerations

Why Not Just Airgap All The Important Control System Networks???

MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

Turn Back The Clock?

Risks & Considerations



MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

Acknowledging Reality

Risks & Considerations

Remote Connectivity & Management Is A Fact Of Existence Now!

MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

While Improving Operations

Risks & Considerations

Remote Connectivity & Management Is A Fact Of Existence Now!

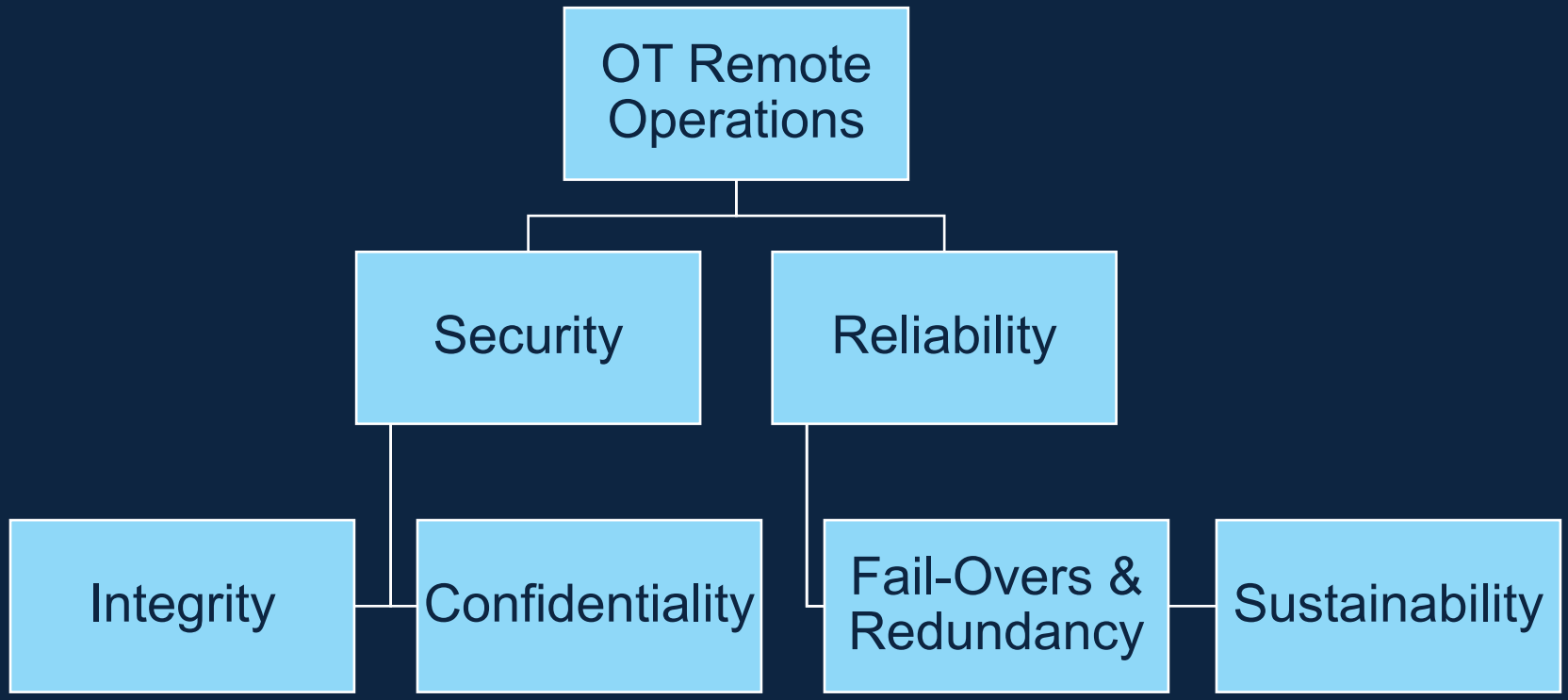
HOWEVER – It CAN & MUST Be Done Securely, Redundantly!

MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

Simplified Planning & Security

Risks & Considerations

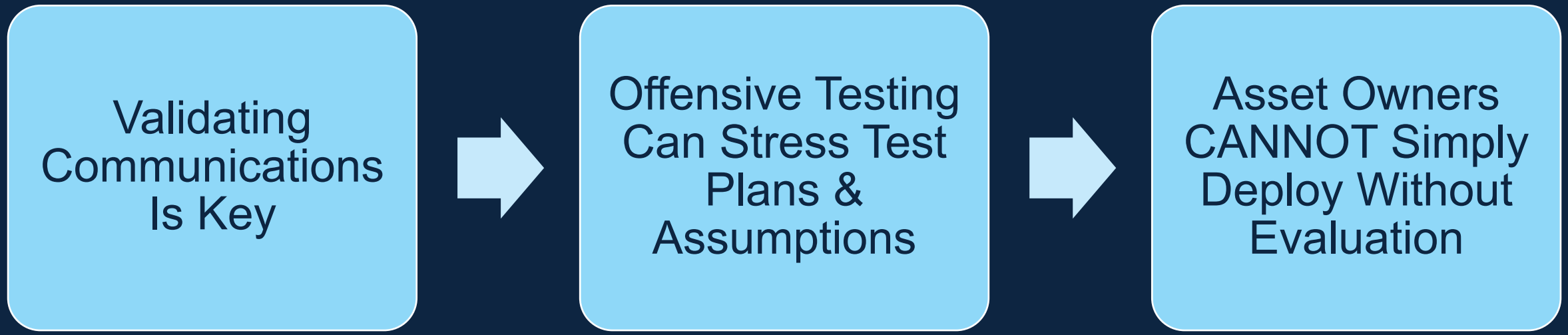


MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

Offensive Security Testing

Risks & Considerations



MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

Additional Considerations

Risks & Considerations



MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

Questions?

MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

Selected Resources

Not A Complete List!

- *“Satellite outage caused 'huge loss in communications' at war's outset -Ukrainian official” – Raphael Satter, Reuters (https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/)*
- *“AcidRain | A Modem Wiper Rains Down on Europe” – Juan Andres Guerrero-Saade & Max von Amerongen, SentinelOne (https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/)*
- *“The Attack on Colonial Pipeline: What We’ve Learned & What We’ve Done Over the Past Two Years” – US Cybersecurity & Infrastructure Security Agency (https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years)*
- *“Cyber attack shuts down U.S. fuel pipeline ‘jugular,’ Biden briefed” – Christopher Bing & Stephanie Kelly, Reuters (https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/)*
- *“Mind the (Air) Gap” - Joe Slowik (https://pylos.co/2021/05/13/mind-the-air-gap/)*

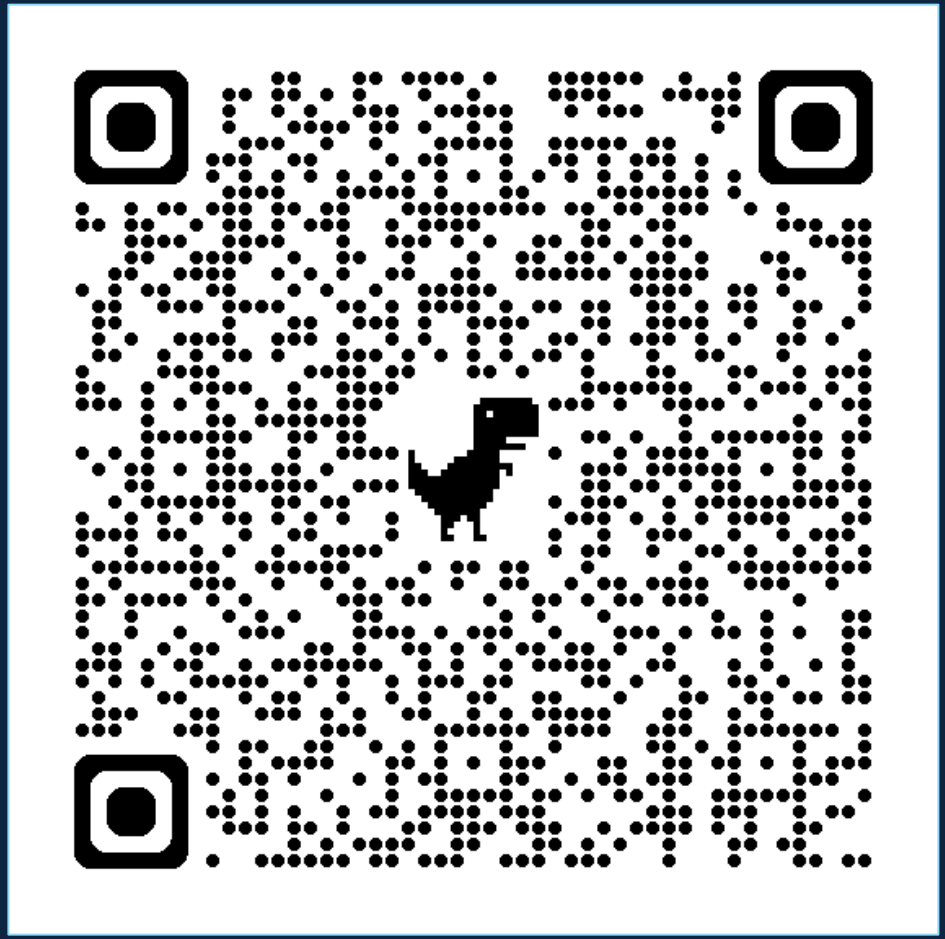
MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

Future KA-SAT Outage Analysis

Stay Tuned!

“Reviewing the 2022 KA-SAT incident & implications for distributed communication environments” - Virus Bulletin 2024 (https://www.virusbulletin.com/conference/vb2024/abstracts/reviewing-2022-ka-sat-incident-implications-distributed-communication-environments/)



MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5

Joe Slowik

jslowik@mitre.org

@JFSLOWIK

https://www.linkedin.com/in/joe-slowik



MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 24-00134-5