MITRE

Building PACE Capabilities for the Current Threat Environment

Implications for Emergency Management and Operational Technology

December 2025

Chris Sledjeski and Mark Bristow

EXECUTIVE SUMMARY

Cyberattacks capable of disrupting multiple interconnected critical infrastructure sectors are possible today.[2, 3] This reality demands additional and, in some cases, divergent Primary, Alternate, Contingency, Emergency (PACE) planning considerations for critical infrastructure operators and emergency managers.

In "blue sky conditions" most emergency management and critical infrastructure operators rely on commercial voice and data communications. Commercial communications infrastructure is highly interoperable, interconnected, and reverse compatible, which makes it highly reliable and efficient under steady-state operating conditions. However, the same interoperability and interconnectedness under systemic cyberattacks means there are shared logical and even physical interconnections that could become chokepoints for regions or systems.

PACE plans should account for cyberattacks that disrupt commercial communications infrastructure including alternate providers of the same commercial communications service. PACE plans also need to account for longer durations (e.g. weeks not days) and wider geographic impacts due to the likelihood of cascading infrastructure failures. Operational plans also need to consider and account for minimum viable operations at each level of communications degradation.

PACE is often thought of as backup communications, but to be durable in the current threat environment, PACE plans must account for a wide range of planning considerations and be supported by real capabilities and capacity. In the context of prolonged and widespread infrastructure disruptions, PACE should include considerations of:

IF YOU CAN'T COMMUNICATE… YOU CAN'T OPERATE.[1]

- Energy (e.g., to support communications and emergency operations)
- Logistics (e.g., dependencies, refueling generators, runners for message relay)
- Staffing and training (e.g., for uncertain conditions and extended durations)
- Planning across multiple levels of administration (e.g., government, other infrastructure operators)
- Security evaluations for each PACE layer (e.g., securing sensitive operational communications across PACE)
- PACE for Industrial Control Systems (ICS) or Operational Technology (OT) critical applications

This white paper—the third in MITRE's ongoing series on critical infrastructure for potential conflict scenarios, as outlined in MITRE's "Five Steps to Prepare Critical Infrastructure for Cyber War"—examines the need to strengthen emergency communications systems. Its purpose is to initiate discussion and promote additional research on strengthening emergency response and recovery for U.S. critical infrastructure under cyberwarfare scenarios. MITRE thanks the infrastructure operators and state and local emergency managers who provided input to this paper.

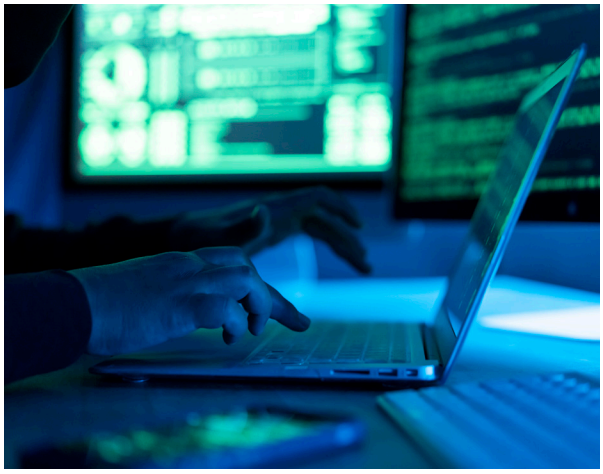
CONTENTS

INTRODUCTION

Participants at MITRE's 2024 classified Critical Infrastructure Cybersecurity (CICS) Tabletop Exercise (TTX)—which convened more than 200 participants from federal agencies, state and local governments, and private-sector operators across 70 organizations—emphasized the need for durable communications alternatives in the current cyber threat environment, regardless of their city, infrastructure sector, or technical discipline.

The CICS TTX validated suspected shortfalls in government and infrastructure operator PACE planning in general, and specifically under multiregional communications and electric outage scenarios. Interviews conducted after the TTX indicated that many infrastructure operators and state and local emergency managers plans are based on flawed assumptions for the current threat environment. These assumptions include misconceptions on the tradeoffs (e.g., reliability, interoperability, security) organizations are making for and across communications alternatives, especially with stakeholders across sectors and jurisdictions. This white paper also provides guidance on PACE implementation considerations for emergency management Operational Technology (OT) applications.

PACE is a methodology for resilient communications.[4] Although PACE is often associated with communications technology, PACE planning must also address supporting factors such as staffing, energy, logistics, and security to be effective. PACE planning typically involves multiple plans for multiple systems or critical



functions within an organization.[5] In an electric utility, for example, business operations, transmission, and distribution operations may need separate but related PACE plans. For a city, region, and the country, PACE implementation needs to occur across multiple levels of administration (e.g., from government, infrastructure operators, individuals), to allow for all these levels to work and coordinate together in a disaster.

OT operators regularly think about resilient communications, however most PACE planning guidance to date has focused on maintaining business communications, and the literature on PACE for ICS or OT is very limited.

PACE PLANNING NEEDS IN 2025

PACE planning in 2025 must account for resilient communications under more extreme conditions than previously envisioned. Most PACE planning in emergency management today, whether in a state/local or infrastructure operator context, addresses natural disaster or terrorist scenarios, which typically manifest randomly and are geographically bound, allowing for substantial mutual aid opportunities. U.S. adversaries, through campaigns like Volt[6] and Salt Typhoon,[7] have the ability and resources to develop and sustain access to critical infrastructure systems that span regions or even the country. This presents a new set of endurance requirements for PACE.

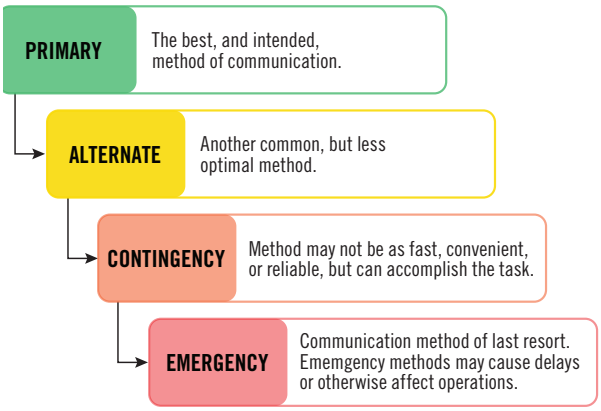


FIGURE 1 CISA PACE PLAN OVERVIEW[8]

Cyber incidents can cascade from a directly impacted network to dependent systems and customers; in some cases, this means regional or national-level impacts, even if the impacts are not enduring. Systemic degradation or loss is fundamentally a different planning scenario than for random, isolated events.[9] Additionally, most existing planning scenarios focus on incidents in a single entity or sector. In this way, cyber exercises and incident planning often fail to exercise the real-world characteristics of cyberattacks on interconnected infrastructure.

Cyber can also come in waves, as Ukraine has experienced since Russia's invasion in February 2022 where there has been a continuing series of wiper attacks on its government and critical industries.[10] The layered characteristic of cyber war attacks surprised TTX participants in how quickly the effects of low-level cyber incidents began to impact critical services when participants accounted for dependencies and interdependencies.

Governments and infrastructure operators already experience lower-level versions of cascading cyber incidents through and across infrastructure sectors. In 2017, Russian military hackers executed a software supply chain attack against Ukrainian tax software, which spread to 65 countries[11] and resulted in over $10 billion in economic damages—the most destructive and costly cyber-attack to date.[12] Not Petya impacted a range of sectors globally, including healthcare, energy, and transportation.[13]

In 2024, an error in a CrowdStrike update to 8.5 million systems shut down services across many industries, including healthcare, travel, and banking, with over $5.4 billion in direct economic impacts.[14] Even natural hazards events, such as Hurricane Helene in 2024, have illustrated the need for PACE improvements. During the storm, 74% of Western North Carolina's cellular sites were down, with some counties experiencing 90% of cellular sites out.[15] The backup 800MHz state network also experienced damage and connectivity issues due to power loss and the inability to refuel all the radio tower generators due to logistics challenges caused by storm debris.

RISKY 2025 PACE PLANNING ASSUMPTIONS

The CICS TTX validated that stakeholders often overestimate the strength of their existing PACE communications plans even under significantly less challenging disruption scenarios. One way this occurs is through a false sense of varied communications.

Most emergency management and critical infrastructure operators rely on commercial voice and data communications. This arrangement is acceptable for Primary and Alternate communications in "blue

sky" or general operating conditions, but it should not be assumed for Contingency and Emergency communications under cyberwarfare conditions.

Commercial communications infrastructure is highly interoperable, interconnected, and reverse compatible, which makes it highly reliable and efficient under steady-state operating conditions. However, the same interoperability and interconnectedness in the context of cyberattacks means there are shared logical and even physical interconnections that could become chokepoints for regions or systems.

A telecommunications circuit leaving an emergency management facility provisioned by one communications company may have to transit another communications company's physical infrastructure. Multiple communications providers may share the same physical or logical infrastructure along a route. As an example for the internet, border gateway protocol attacks, which leverage internet routing vulnerabilities, have the potential to disrupt nation-wide internet connectivity, at least for a period.

The CICS TTX reminded participants that they should not assume that PACE fundamentals have been taken care of. Numerous emergency managers and utilities remarked that they were not certain whether hard copy lists of phone and Emergency communications information were complete or up to date. Some noted that they did not keep physical copies of procedures or contact information anymore. Indeed, many organizations rely on a common internet-based incident management application to maintain situational awareness, which may not be available, depending on local configuration, where commercial communications are lost or significantly degraded.

TTX participants also raised best practices—a daily update to emergency communications rosters pushed to every company location for local area access or printing. Updated physical document references may seem outdated in 2025, but they can provide outsized value in PACE plans that account for widespread disruptions of communications and information technology (IT) services.

COMMUNICATIONS PLANNING ACROSS PACE

PACE implementation across an organization, whether for IT or OT purposes, should employ a variety of methods—in transmission media and communications modalities.[16] It is also important to recognize that the volume and functionality of communications an organization can sustain will decrease substantially and non-linearly from Primary (P) to Emergency (E) modes. Important tradeoffs on critical voice, IT, and OT data needs are required and should be accounted for now in operations plans.

Primary is exactly that—an organization's primary means of communications. In a business network, this may be commercially provided communications; an OT environment may also rely on commercial communications to support ICS/Supervisory Control and Data Acquisition (SCADA) network control and data polling needs. Alternate communications should account for at least a single failure in a primary network or application. A separate telecommunications provider is acceptable as Alternate in a PACE plan.

In contrast, Contingency communications planning should account for the possibility of system-wide outages (e.g., 5g and 4g networks with shared infrastructure between providers). Services like Government Emergency Telecommunications Service (GETS)[a], Wireless Priority Service (WPS), and Telecommunications Service Priority (TSP)[b] are still

a Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) are White House-directed emergency telephone service provided and managed by CISA. (available at https://www.cisa.gov/resources-tools/services/government-emergency-telecommunications-service-gets and https://www.cisa.gov/resources-tools/services/wireless-priority-service-wps)

b Telecommunications Service Priority (TSP) is a Federal Communications Commission (FCC) program, managed by CISA, which mandates that service providers prioritize voice and data circuits provisioning and restoration requests made by organizations with national security and emergency preparedness missions. (available at https://www.cisa.gov/resources-tools/services/telecommunications-service-priority-tsp)

recommended steps for critical infrastructure entities, but they are not a guarantee of service—particularly under a systemic cyberattack on a communications provider or providers. For example, adversary capabilities exist today that can impact multiple communications providers. An attack on Border Gateway Protocol (BGP) via BGP hijacking could cause legitimate services to become unreachable, causing outages for many providers and users across the internet at the same time.[17]

Satellite communications (SATCOM) are acceptable as one type of Contingency communications option, but in conversations with industry communications experts, SATCOM should not be assumed for Emergency communications under PACE in the current threat environment. The next section describes some of the limitations of SATCOM as an Emergency communications medium.

SATCOM DEPENDENCIES AND LIMITATIONS

Like terrestrial communications, if there are multi-region or widespread communications issues, users with SATCOM will suddenly move to this communications medium, potentially overwhelming this already more constrained communications type. Despite its name, SATCOM typically has substantial terrestrial dependencies on the telecommunications system. Communications traffic is sent up and down through ground stations or hubs and routed, where possible, mostly through terrestrial networks.[18] Satellite communications are often inherently tied to telecommunications ground infrastructure that depends on electricity and connectivity to the terrestrial network. SATCOM is also increasingly dependent on cloud infrastructure,[19] which in turn requires cloud and IT services functioning, telecommunications, and electrical infrastructure. There are also known and emerging cyber and radio frequency (RF) capabilities against SATCOM, for example, those reported by ViaSat in the 2022 Acid Rain incident that should be accounted for under crisis and conflict scenarios.[20, 21]

EMERGENCY COMMUNICATIONS

When an organization has reached Emergency communications, the E in their PACE plan, they should assume all standard commercial IP traffic and communications are unavailable in a wide area. Communications will be drastically reduced at this point, and it will take significantly longer to coordinate and complete essential tasks than most existing PACE plans account for. One infrastructure operator, when asked about Emergency communications said, "we would use runners." This is a feasible response in a geographically bound area where people have been trained and identified to relay messages through a known set of relay points and procedures, but it may not be feasible at scale and duration without substantial staffing and resources. More likely than not, there will be a need for a mesh of alternate communications along with relay procedures.

PRE-DEVELOPING OPERATIONS PLANS FOR VARYING LEVELS OF COMMS DEGRADATION

Operational plans also need to consider and account for minimum viable operations at each level of communications degradation. A risk assessment that identifies the specific operational dependencies on communication systems at each level—Primary, Alternate, Contingency, and Emergency—helps organizations understand how the degradation and loss of communications across their PACE plans will affect mission-critical tasks. For example, if an organization relies on commercial communications and then switches to satellite communications, there are only so many satellite receivers and bandwidth available. A risk assessment would identify what priority communications are available at that point of degradation, who and what roles will access those communications, and in what locations, to accomplish a minimum required set of activities. The assessment should also identify what range of communications delays are tolerable in these varied PACE configurations, which also informs technical requirements for PACE communications.

TTXS TO SORT OUT THE LOGISTICS OF PACE

PACE plans, whether for IT or OT functions, require identifying and training a workforce that can implement them under uncertain conditions and durations that may exceed current planning horizons (e.g., weeks versus days). Most participants at the CICS TTX acknowledged that their organizations rarely practiced or allotted sufficient annual training to their PACE plans. PACE training exercises should consider a mix of ongoing internal communications drills, tabletop exercises, or more involved, full-scale exercises—ideally with key external dependency organizations.[22] Annual or quarterly exercises can only mature an organization's PACE plan so far. Consider practicing PACE through weekly mini-drills for all shifts. Have employees practice calling a site on a different communications medium. Have control center staff validate the PACE contact information for a critical partner and practice calling that partner on an emergency communications connection. More frequent PACE plan tests build organizational muscle memory. Cross-organizational tabletop exercises help identify bottlenecks in information flows and decision making and point to mitigation strategies, such as pre-authorized decision trees or decentralized command structures.

PACE plans also need to account for backup power for all communications modalities across PACE. Additionally, PACE plans should incorporate triggers to inform participants of the current PACE condition under which they are operating. These triggers should include procedure-based actions tied to operating conditions, since consistent communication may not always be possible (e.g., if a message from the control center has not been received within X hours, the participant will perform Y or send someone to the control center for further instructions). PACE should account for the need to staff these plans for extended periods (e.g., weeks) of time under uncertain conditions.

Further, consider PACE plan provisions for how to quietly shift to out-of-band communications when there are concerns that cyber actors may be present in networks or in response to established threat-based signposts for the general operating environment (e.g., if geopolitical event X occurs move operations discussions to Y communications network).

CROSS-SECTOR PACE PLANS ARE A MUST

If an organization does not coordinate its PACE plan with its cross-sector dependencies, PACE plans are incomplete, and they will fail sooner than necessary. In the CICS TTX, Electric, Pipeline, and Communications sector personnel acknowledged the criticality of their ongoing PACE planning efforts, but they acknowledged that cross-sector PACE planning was not uniform across jurisdictions and sectors. Planning and exercises should test the interoperability of PACE plans between the infrastructure operators, key dependencies, and government because restoration and recovery will require coordinated actions between sectors under constrained communications.

PACE FOR OPERATIONAL TECHNOLOGY?

There is scant and inconsistent guidance in open-source literature on how PACE could be applied to OT environments. Few have considered extended and wide-scale infrastructure disruption planning scenarios for OT communications. This may be driven by an assumption that during widespread power outages, operations will simply be down. The CICS TTX participants identified scenarios in which OT PACE plans would be valuable. For example, electric power may be stable, but commercial communications could be substantially degraded. Another scenario considered was that emergency backup power lasts for a period, but Primary and Alternate communications circuits are unavailable or become unavailable as backup generator fuel is contested.

OT elements seeking to develop PACE plans should identify (a) the critical functions supported by Primary, Alternate, Contingency, and Emergency communications; (b) the functions enabled by the backup alternatives; and (c) the degree to which

operations can continue under the alternatives. In some ways, supporting the communications needs of OT are easier in that the data volume requirements are generally lower. SCADA systems typically poll, or request, new information about every 2–4 seconds.[23] Most ICS devices require very little bandwidth, for example, around 10 megabits per second (Mbps) for PLCs and RTUs, but they do require low latency and jitter.[24] ***Appendix A: Example of PACE Considerations for Industrial Control System Functions*** provides a sample of OT communications quality of service and compatibility considerations.

Organizations will need to make tough choices around the absolute minimum of communications required for essential OT functions. Limitations in the bandwidth, speed, and behavior of Contingency and Emergency communications employed in OT will also determine which OT communications protocols and functions can be supported. In general, any real-time communications, such as those that might be found in protective relays that require precise and high-speed coordination, are unlikely to be supported by more austere alternative communication types.

Under steady-state conditions, OT systems may receive thousands of data points per minute; however, the same system may be able to be configured to safely operate fewer data points at extended periods. In conversations with infrastructure operators, assuming the ICS/SCADA is still functioning in its baseline configuration (e.g., no cyber degradation to network or controllers), many said it would be possible to continue to operate with tradeoffs in efficiency and reliability. This same scenario may not be possible for all sector functions or for distributed control systems (DCS),but they are typically geographically constrained (e.g., building, site, complex).

COMMUNICATION SECURITY ACROSS PACE

PACE communication security evaluations should assess both the security and reliability of the communication methods used in each layer of the PACE plan. Maintaining the same level of security in communications may become increasingly challenging at the Contingency (C) and Emergency (E) levels.

Security evaluations should consider the ability to operate securely in degraded or contested environments. There will be tradeoffs across PACE, but Emergency communications can still be secure and effective. One low-tech solution that could be implemented for some functions is to use pre-shared codebooks, which allow participants to communicate openly without exposing sensitive information.

CONCLUSION

Today, cyberattacks can impact multiple interconnected critical infrastructure sectors across multiple cities for potentially weeks at a time. This possibility demands additional and, in some cases, divergent PACE planning considerations. The cyber disruption potential from access campaigns such as Volt and Salt Typhoon show organizations the substantive difference between cyber capabilities and capacity now versus the decade and a half of government and industry warnings on adversarial interest in conditional disruption of critical infrastructure systems.[25, 26, 27]

PACE planning is about resilience. The current threat environment demands a substantial evolution of PACE plans and capacity against adversary disruptive capabilities to improve resilience outcomes for critical infrastructure in a cyberwar.

APPENDIX A

EXAMPLE OF PACE CONSIDERATIONS FOR INDUSTRIAL CONTROL SYSTEM FUNCTIONS

Alternative Communications		Quality of Service Requirements (Approximated)				ICS Protocol Requirements						
Type	Radio Frequency Band[28]	Range (miles)	Bandwidth	Jitter	Latency	Modbus	IEC-104	ICCP	IEC 61850	DNP3	OPC	OPC-UA
2G Cellular	UHF	1 – 10	Low to Moderate (10– 400 Kbps)	Moderate (30– 100 ms)	Moderate (150– 300 ms)	YES	NO	NO	NO	YES	NO	NO
3G Cellular	UHF	1 – 10	Moderate to High (200– 42 Mbps)	Low to Moderate (10– 50 ms)	Low to Moderate (100– 200 ms)	YES	YES	YES	YES	YES	YES	YES
HF Radio	Shortwave	3,000+	Low (3– 240 Kbps)	Moderate to High (100– 500 ms)	High (500 ms– 2 sec)	YES	NO	NO	NO	YES	NO	NO
Shortwave	HF	3,000+	Low (3– 240 Kbps)	High (100– 500 ms)	High (500 ms– 2 sec)	YES	NO	NO	NO	YES	NO	NO
Satellite	SHF	Global (virtually unlimited)	High (up to 250 Mbps or more)	Low to Moderate (30– 600 ms)	Moderate to High (500 ms– 1 sec)	YES	YES	YES	YES	YES	YES	YES
UHF Radio	UHF	2 – 50	Moderate (12 Kbps– Mbps)	Moderate (5– 30 ms)	Low to Moderate (1– 10 ms)	YES	NO	NO	NO	YES	NO	NO
VHF Radio	VHF	2 – 50	Low to Moderate (10– 56 Kbps)	Moderate (5–30 ms)	Low to Moderate (1–10 ms)	YES	NO	NO	NO	YES	NO	NO

ACKNOWLEDGMENTS

The author would like to thank the infrastructure operators and state and local emergency managers who provided input to this paper and to Nick Tsamis and Tony Webber for their thoughtful input and review of this document

ENDNOTES

1 Cybersecurity and Infrastructure Security Agency, "Introduction to PACE Planning for the Emergency Communications Ecosystem," April 2025. https://www.youtube.com/watch?v=R5Tm7Tt2eXw.

2 Director of National Intelligence, "Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee," 29 January 2019. [Online] Available: https://www.intelligence.gov/assets/documents/archive/2019-ATA-SFR---SSCI.pdf.

3 Director of National Intelligence, "Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee," March 2025. [Online] Available: https://www.odni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.

4 Cybersecurity and Infrastructure Security Agency, "Leveraging the PACE Plan into the Emergency Communications Ecosystem," October 2024. [Online] Available: https://www.cisa.gov/sites/default/files/2024-10/2024_NCSWICPTE_Leveraging_PACE_Plan_Emergency_Comms_Ecosystems.pdf.

5 Cybersecurity and Infrastructure Security Agency, "Introduction to PACE Planning for the Emergency Communications Ecosystem," April 2025. https://www.youtube.com/watch?v=R5Tm7Tt2eXw.

6 Cybersecurity and Infrastructure Security Agency, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," 7 February 2024. [Online] Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

7 Cybersecurity Dive, "White House Says 9th Telecom Company Hit in Salt Typhoon Spree," 27 December 2024. [Online] Available: https://www.cybersecuritydive.com/news/salt-typhoon-telecom-attacks-lax-security/736233/.

8 Cybersecurity and Infrastructure Security Agency, "Leveraging the PACE Plan into the Emergency Communications Ecosystem," October 2024. [Online] Available: https://www.cisa.gov/sites/default/files/2024-10/2024_NCSWICPTE_Leveraging_PACE_Plan_Emergency_Comms_Ecosystems.pdf.

9 Barabási, Albert-László. Linked: The New Science of Networks. Perseus Pub., 2002.

10 ESET, "A year of wiper attacks in Ukraine," 24 February 2023. [Online] Available: https://www.welivesecurity.com/2023/02/24/year-wiper-attacks-ukraine/.

11 USA Today, "Petya cyberattack spreads to 65 countries," 28 June 2017. [Online] Available: https://www.usatoday.com/story/tech/talkingtech/2017/06/28/petya-cyberattack-spreads-65-countries/435016001/.

12 The White House, "Statement from the Press Secretary," 15 February 2018. [Online] Available: https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/.

13 Claroty, "NotPetya: Looking Back Six Years Later," 6 June 2023. [Online] Available: https://claroty.com/blog/notpetya-looking-back-six-years-later.

14 Information Week, "CrowdStrike Outage Drained $5.4 Billion From Fortune 500: Report," 30 July 2024. [Online] Available: https://www.informationweek.com/cyber-resilience/crowdstrike-outage-drained-5-4-billion-from-fortune-500-report.

15 Hagerty Consulting, Inc., "Coordinating Through Crisis: Resilient Communications Hurricane Helene Case Study," 2025. [Online] Available: https://nerc123.my.salesforce.com/sfc/p/#2E0000012tgy/a/Pm000003jpkb/xSntV3Htv2c2eMbcUG_Cy6xQKR5C0PEPOM9LALg4gfI.

16 Cybersecurity and Infrastructure Security Agency, "Leveraging the PACE Plan into the Emergency Communications Ecosystem," October 2024. [Online] Available: https://www.cisa.gov/sites/default/files/2024-10/2024_NCSWICPTE_Leveraging_PACE_Plan_Emergency_Comms_Ecosystems.pdf.

17 Cloudflare, "What is BGP hijacking?," [Online] Available: https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/#:~:text=As%20a%20result%20of%20BGP,in%20order%20to%20steal%20credentials.

18 Government of Canada, "Satellite communications - ITSAP.80.029," March 2023. [Online] https://www.cyber.gc.ca/en/guidance/satellite-communications-itsap80029.

19 Medium, "Cloud Control: How Cloud Computing Is Revolutionizing Space Operations," 30 April 2024. [Online] Available: https://medium.com/@leontyron/cloud-control-how-cloud-computing-is-revolutionizing-satellite-space-operations-679317d31701

20 SentinelLABS, "Acid Rain | A Modem Wiper Rains Down on Europe," 31 March 2022. [Online] Available: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/.

21 Cyberscoop, "Satellite hack on eve of Ukraine war was a coordinated, multi-pronged assault," 10 August 2023. [Online] Available: https://cyberscoop.com/viasat-ka-sat-hack-black-hat/

22 Environmental Protection Agency, "Water Sector Guide to Telecommunications During Power Outages," June 2022. [Online] Available: https://www.epa.gov/system/files/documents/2022-06/TelecomGuide_508c.pdf.

23 Blume, Steven W. Electric Power System Basics for the Nonelectrical Professional. p189. 2nd ed., Wiley-IEEE Press, 2016.

24 Knapp, Eric D. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. p120. 3rd ed., Syngress, 2024.

25 Director of National Intelligence, "Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee," 27 February 2008. [Online] Available: https://www.intelligence.gov/assets/documents/archive/20080227_testimony.pdf.

26 Director of National Intelligence, "Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee," 29 January 2019. [Online] Available: https://www.intelligence.gov/assets/documents/archive/2019-ATA-SFR---SSCI.pdf.

27 Director of National Intelligence, "Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee," March 2025. [Online] Available: https://www.odni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.

28 TeraSense, "Radio Frequency Bands," 2 September 2025. [Online] Available: https://terasense.com/terahertz-technology/radio-frequency-bands/

MITRE