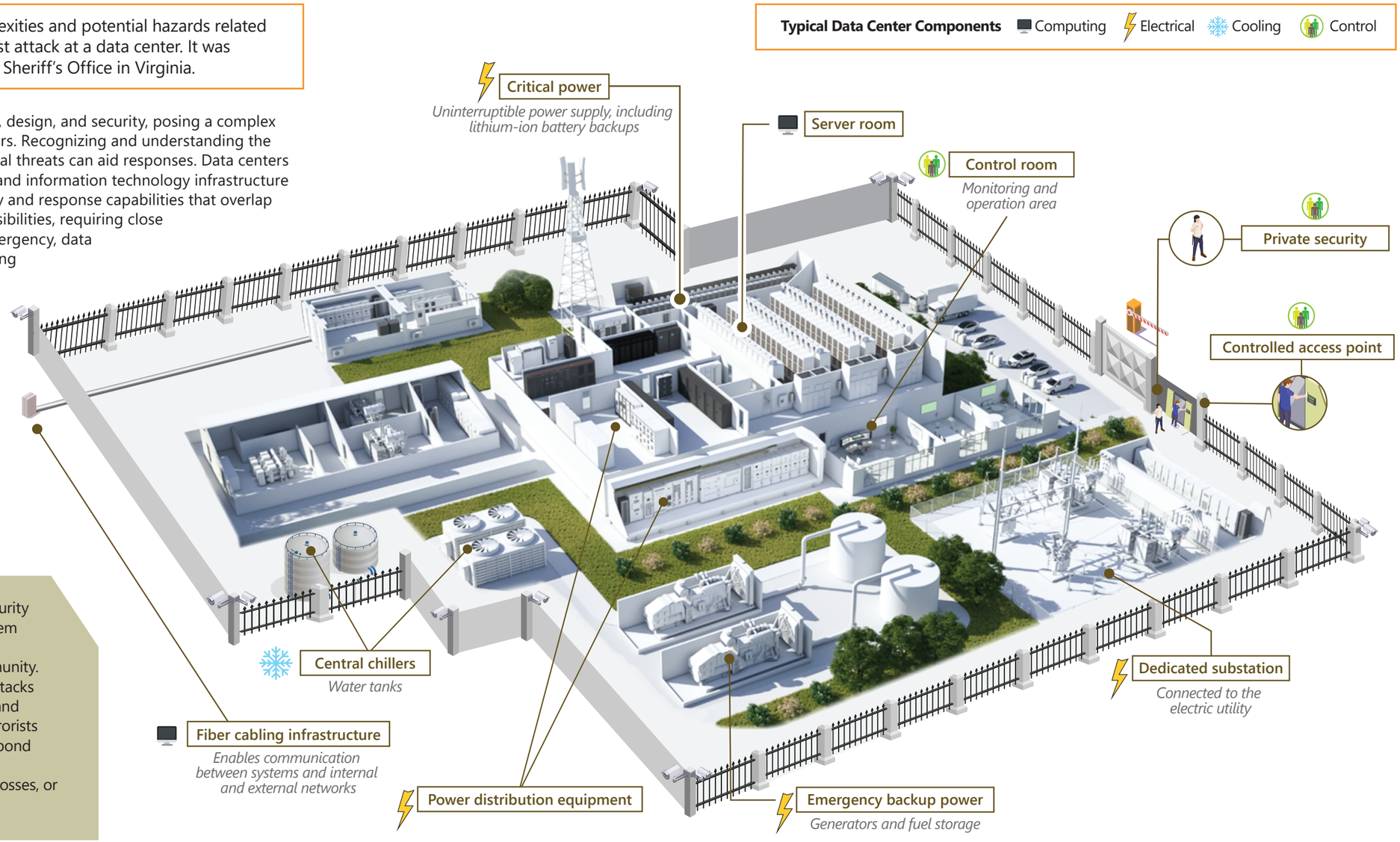
Complex Operating Environment – Data Centers

SCOPE: This product highlights complexities and potential hazards related to an emergency response to a terrorist attack at a data center. It was coordinated with the Loudoun County Sheriff's Office in Virginia.

Data centers vary greatly in size, location, design, and security, posing a complex operating environment for first responders. Recognizing and understanding the components of a data center and potential threats can aid responses. Data centers and the energy, water, communications, and information technology infrastructure they rely on often have their own security and response capabilities that overlap with first responder jurisdictional responsibilities, requiring close coordination with stakeholders. In an emergency, data center personnel can assess their operating systems and components to restore essential services; however, they may not be trained to deal with complex cyber or physical terrorist attacks.

The convergence of cyber and physical security threats to the growing data center ecosystem creates significant challenges for security stakeholders and the first responder community. Terrorists may conduct physical or cyber attacks on data centers or against the employees and infrastructure that support the centers. Terrorists might use such attacks to create panic, respond to perceptions of government overstep or environmental concerns,[a] inflict economic losses, or retaliate for US military actions abroad.



[a]The mere advocacy of or membership in groups that promote political or social positions, political activism, the use of strong rhetoric, or the generalized philosophical embrace of violent tactics does not necessarily constitute violent extremism and may be constitutionally protected. Such use of strong rhetoric and divisive terms should not be assumed to reflect further violent extremist activity, absent additional information, and should be considered in the context of all applicable laws and policies regarding privacy, civil rights, and civil liberties.

(U) NOTICE: This is a Joint Counterterrorism Assessment Team (JCAT) product. JCAT is a collaboration by NCTC, DHS, FBI, and state, local, tribal, and territorial government personnel to improve information sharing and enhance public safety. The product promotes coordination among intergovernmental authorities and the private sector in identifying, preventing, and responding to terrorist activities. Consider the enclosed information within the context of existing laws, regulations, authorities, agreements, policies, or procedures. For additional information contact us at JCAT@ODNI.GOV. This document is best printed on 11"×17" paper.

NCTC-JFRT-2026-15754
10 NOVEMBER 2026
AUTHORED BY NCTC, DHS, FBI

Complex Operating Environment – Data Centers *(continued)*

PHYSICAL THREATS

Physical threats to data centers and support infrastructure have historically involved low-technology methods, including small-arms fire, sabotage, arson, and explosives. However, FTOs have attacked US-owned data centers abroad with UAS. Differentiating a terrorist attack from a criminal act may be challenging at both the response and investigation stages. Public safety community and industry professionals are well positioned to detect threats to data centers and supporting infrastructure. Indications of a physical attack or plotting by terrorists or criminals may include the following:

- Theft of equipment, uniforms, or identification cards
- Presence of unauthorized individuals or vehicles at a restricted site or adjacent area, such as an electric substation or underground utility
- Threats of violence related to data centers or attempts to justify such violence communicated in person or online
- Probing of security or unusual, repeated, or prolonged visits to the site or adjacent areas, including taking photographs or possessing maps or blueprints without a valid reason
- Disruption of perimeter fencing or other physical security measures or evidence of intrusion, such as cut locks or triggered alarms
- Modified UAS or unusual UAS activity above or near a data center
- Unexplained disruption of power, water, or communications services
- Explosions or suspected IEDs
- Sound of gunfire or observed ballistic damage to a data center or supporting infrastructure once the threat of an active shooter is diminished
- Fire damage or smoke, possibly indicating arson or an incendiary device

PERSONNEL

Law enforcement and security stakeholders should maintain awareness of threats of violence against data center employees and government officials who are perceived to be tied to data center legislation and approvals while protecting constitutional rights.

As with any large gathering of people, terrorists may attempt to exploit lawful public assemblies—such as protests, rallies, or demonstrations against data center infrastructure growth—by attacking attendees or crowds or trying to incite protestors or super intelligence[b] opposition groups to violence. Awareness of the complexities associated with public assemblies and the additional threats of terrorist exploitation can improve public safety personnel's preparedness and response. Public assembles may be driven by world events; draw large numbers of participants, spectators, and opposition; and start spontaneously. Terrorist exploitation of a public assembly may have impacts beyond the immediate location, for example prompting an increase in security at other critical infrastructure sites.

Data centers may be targets of insider threats, such as an employee who provides facility access or sensitive information to an adversary. Insider threats can begin as early as the job application process, when adversaries may direct applicants to seek employment with access to facility layouts, site security, intellectual property, and customer information. Terrorists may target US data center employees for attacks or recruitment as inside sources.

CYBER THREAT

Owners and operators are most likely to detect a cyber attack against a data center. Such attacks might include phishing emails containing malware to gain unauthorized access to a facility's servers or industrial control systems, ransomware, efforts to steal personally identifiable information and other data, and credential abuse. Some data center companies may be reluctant to report malicious cyber incidents to law enforcement because of the potential for reputational harm or economic loss. Proactive law enforcement outreach to the private sector may foster cooperative relationships and enhance threat information sharing.

RESPONSE CONSIDERATIONS

To render the site safe to enter, first responders should contact and coordinate with the facility's owner and operator for help with onsite access upon discovery of possible tampering; sabotage; or damage to equipment or surrounding energy, water, communication, or information technology infrastructure. To save time during an incident, know beforehand what equipment is already on site, and be prepared to bring in appropriate tools to avoid multiple runs to emergency vehicles. First responders might encounter the following potentially hazardous scenarios and complexities during incident response:

- **Security and Access:** Data centers are usually secure facilities, with restricted, hardened inner and outer perimeters that can hinder emergency response ingress and egress. First responders and emergency managers should tour the facilities to get familiar with their layout, size, security access protocols, and facility points of contact in case of an incident. Team up with data center security and engineering teams trained to assist first responders in more efficiently navigating the facility.
- **Communications:** Data centers' partially underground construction and steel and concrete components may block radio frequency transmission and cellular network connectivity in and around facilities. Testing radios, cell phones, and secure communications during tours or exercises may better prepare first responders to have interoperable systems and access to backup communications during calls for service.
- **Lithium-ion batteries:** Data center backup power systems, such as an uninterruptible power supply, often contain large lithium-ion battery banks. If ignited by an attack or sabotage, these batteries can experience a "thermal runaway," a self-escalating reaction causing intense fires, explosions, and the release of toxic gases and hydrogen, which can reignite.
- **Electrical (Energized) Equipment:** Data centers use immense amounts of electrical power. First responders face the danger of electrical shock from high-voltage cables, power distribution units, and battery storage units, even if the main power is off.
- **Hidden Fire Spread:** Fires can travel through hard-to-access areas, such as under-floor (used for cooling and cabling) or above-ceiling spaces, making locating the seat of the fire difficult.
- **Reduced Visibility and Toxic Smoke:** Fires in these environments often produce thick, black smoke from burning plastic insulation and cabling, reducing visibility for interior crews and creating possible respiratory hazards.
- **Suffocation Risks:** Data centers are usually equipped with advanced fire suppression systems that work by displacing oxygen levels. These systems are designed to protect electronic equipment, but an unexpected discharge could pose a suffocation risk to personnel.
- **Structural Damage:** Overheated equipment can fail, causing structural components to fall or sustain damage.

REPORTING AND INFORMATION SHARING

Ensure reporting criteria, thresholds, and processes are established and implemented consistently so that suspicious activity and incidents are reported in a timely manner. The Nationwide Suspicious Activity Reporting Initiative provides education on suspicious activity reporting (SAR) and SAR mechanisms.

Ensure that data center, supporting critical infrastructure, public safety, emergency management, and Federal Government liaisons communicate regularly and collectively report and share information about suspicious activity concerning infrastructure that may have cascading impacts to data centers. Maintain relationships between the private and public sectors, for example by training at data centers and utility facilities through tours and exercises and by developing a common terminology to describe threats and response capabilities. Such measures will improve first responder knowledge of data center facilities, helping to expedite response and ensure safety during an incident.

First responders should work with owners and operators, relevant state regulators, and fusion centers to ensure mutual awareness regarding the reporting of suspicious activity, including:

- Benchmarks and suspicious reporting thresholds
- Incident timelines and facts
- Priorities for both the private sector and law enforcement
- Availability and replacement time frame of on-site equipment for use during or after an incident

RESOURCES

JCAT First Responder's Toolboxes provide information about terrorist tactics and response and mitigation considerations. The hyperlinked products, some of which are FOUO, can also be found on JCAT's website, DHS's Homeland Security Information Network, or FBI's Law Enforcement Enterprise Portal.

[b] Previously referred to as artificial intelligence

(U) NOTICE: This is a Joint Counterterrorism Assessment Team (JCAT) product. JCAT is a collaboration by NCTC, DHS, FBI, and state, local, tribal, and territorial government personnel to improve information sharing and enhance public safety. The product promotes coordination among intergovernmental authorities and the private sector in identifying, preventing, and responding to terrorist activities. Consider the enclosed information within the context of existing laws, regulations, authorities, agreements, policies, or procedures. For additional information contact us at JCAT@ODNI.GOV. This document is best printed on 11"×17" paper.

NCTC-JFRT-2026-15754

10 NOVEMBER 2026
AUTHORED BY NCTC, DHS, FBI

JCAT

JOINT COUNTERTERRORISM ASSESSMENT TEAM

PRODUCT FEEDBACK

Please use the link below to complete a short survey. Your feedback will help JCAT develop counterterrorism products that support the public safety and private sector community.

https://www.JCAT-url.com

For further information, please email JCAT
jcat@odni.gov

(U) The Joint Counterterrorism Assessment Team (JCAT) is a collaboration by NCTC, DHS, FBI, state, local, tribal, and territorial government personnel to improve information sharing and enhance public safety. The First Responder's Toolbox is an ad hoc, unclassified reference aid intended to promote counterterrorism coordination among federal, state, local, tribal, and territorial government authorities and partnerships with private sector officials in deterring, preventing, disrupting, and responding to terrorist attacks.