



CROSSROADS • ISSUE 1 • MAY 3, 2026 • ~10 MIN READ

The Critical Infrastructure Behind the World's Biggest Events

1. When the world shows up at one address
2. The infrastructure stack behind a major event
3. What operates inside a modern venue
4. Historical activity: from disruption to scale
5. Recurring threat patterns in public reporting
6. Themes highlighted in public guidance
7. Sources

This issue examines the infrastructure layers behind major events, the systems that operate within them, historical cyber activity tied to similar environments, and themes highlighted in public reporting ahead of FIFA World Cup 2026 and the Miami Formula 1 Grand Prix.

When the world shows up at one address

Events such as the FIFA World Cup, Formula 1 race weekends, and the Olympic Games concentrate population, infrastructure, and digital systems into a tightly bounded footprint. The result is a temporary environment that shares many characteristics with a metropolitan area, but operates on compressed timelines and with less margin for disruption.

Within that footprint:

- Power demand fluctuates rapidly and predictably around event timing
- Water and wastewater systems operate at peak throughput
- Transportation and aviation systems coordinate at regional scale
- Broadcast and telecommunications systems deliver globally visible outputs
- Building and venue OT systems manage the physical environment in real time

Because of their visibility and symbolic value, these events are frequently referenced in public reporting as potential focal points for cyber and physical disruption.

The infrastructure stack behind a major event

Stripped of branding, a large-scale event relies on a layered infrastructure model similar to that of a city — condensed in both space and time.

**Figure 1 · Event Infrastructure Stack**

Figure 1: Event Infrastructure Stack. Major events concentrate public-facing systems, venue OT, telecommunications, mobility, and foundational infrastructure into a temporary high-density operating environment.

Electric power and energy systems. Venue operations — including lighting, HVAC, broadcast equipment, and concessions — depend on local utilities, often supplemented by backup generation and power-conditioning systems. Public case studies highlight specialized distribution technologies used to support communications and in-venue connectivity, such as [VoltServer's Digital Electricity platform at Hard Rock Stadium](#)¹. Organizations operating within regulated environments may align their security posture with frameworks such as NERC CIP, depending on their role in supporting infrastructure.

Water, wastewater, and cooling systems. Large venues process significant volumes of water and wastewater over short periods. Public reporting around recent events has noted that [multiple water systems are often included within cybersecurity planning scope](#)², reflecting their operational importance.

Transportation and mobility systems. Host regions coordinate across transit agencies, traffic systems, and airports. [Reporting on recent event planning](#)³ has described multi-agency collaboration involving utilities, transportation authorities, and law enforcement.

Broadcast, telecommunications, and digital platforms. Broadcast infrastructure, mobile applications, ticketing systems, and in-venue connectivity represent some of the most visible components of event infrastructure. These systems have historically appeared in public reporting on disruptive cyber activity due to their direct impact on the audience experience. Hard Rock Stadium, for example, runs a [Verizon 5G Private Network](#)⁴ for the Miami Grand Prix and recently moved to a [unified Verkada cloud platform](#)⁵ covering its physical security footprint.

Venue operational technology (OT). The venue itself functions as a complex automation environment, integrating building systems, safety controls, and digital infrastructure into a unified operational layer.

What operates inside a modern venue

[Industry materials](#)⁶ and [vendor documentation](#)⁷ describe modern venues as highly dynamic environments capable of scaling from minimal occupancy to full capacity in a short period of time.

A representative OT footprint may include:



- Building automation and management systems (BAS / BMS)
- HVAC control systems and actuators
- Environmental and occupancy sensing
- Networked lighting systems
- Field and turf management systems
- Fire detection and life safety systems
- Physical access control and credentialing
- Video surveillance platforms
- Distributed antenna systems (DAS)
- Concessions and refrigeration automation
- Parking and ventilation systems
- Broadcast production infrastructure

Many of these systems are network-connected and, depending on architecture, may interface with enterprise IT or external services. This convergence between traditionally isolated systems and broader networks is frequently discussed in public cybersecurity research.

Historical activity: from disruption to scale

Cyber activity associated with major events has been documented across multiple public sources.

PyeongChang 2018 (Olympic Destroyer). Public analyses describe a [coordinated disruption affecting IT systems](#)⁸, including domain controllers, ticketing infrastructure, and venue connectivity. The [incident is often referenced](#)⁹ as an example of activity timed for maximum global visibility, with [downstream effects also reported at supporting venues](#)¹⁰.

Paris 2024. After-action reporting from organizations including [ANSSI and the Cyber Threat Alliance](#)¹¹ documented a high volume of cyber events, with a smaller subset resulting in confirmed access. Public summaries emphasized both the [scale of monitoring and the breadth of deployed defensive systems](#)².

World Cup 2026 outlook. [Public risk outlooks](#)¹² and [reporting](#)¹³ have identified recurring categories such as phishing, distributed denial-of-service (DDoS), fraudulent websites, disinformation, and ransomware. Some reporting also notes the potential for activity affecting supporting infrastructure, including energy and water systems. Organizations such as [CISA have publicly described ongoing engagement, exercises, and assessments](#)¹⁴ in preparation for the event, including [a Region 4 tabletop exercise hosted by the City of Miami](#)¹⁵.

Recurring threat patterns in public reporting

Across historical analysis and current outlooks, several patterns appear consistently:

- Credential-focused phishing and supplier-targeted campaigns
- Lookalike domains and fraudulent ticketing platforms
- DDoS activity targeting public-facing systems
- Disinformation and synthetic media aligned with event timelines
- Ransomware affecting supporting services
- Mobile and application-layer threats
- Potential targeting of supporting infrastructure systems



These patterns are widely documented and tend to scale with the visibility of the event.

Themes highlighted in public guidance

After-action reports and public guidance frequently emphasize several areas of focus:

- Scenario-based exercises centered on service disruption
- Visibility into contractor and third-party access
- System resilience and fallback capabilities
- Coordination between infrastructure operators and emergency management
- Preparedness for attacks against public-facing systems

Regulatory and compliance discussions have also highlighted areas such as third-party risk, cloud integration, and distributed energy resources as ongoing considerations.

Sources

- White House FIFA World Cup 2026 Task Force¹⁴
- Politico — How hackers could disrupt the World Cup (Apr 12, 2026)³
- Linden NJ — FIFA World Cup 2026 Cyber Threat and Risk Outlook¹²
- City of Miami — Region 4 Miami World Cup Tabletop Exercise (Jan 28, 2026)¹⁵
- Cyber Threat Alliance — Paris Olympics After-Action Report¹¹
- Nozomi Networks — Protecting the 2024 Paris Olympics²
- Dataminr — Preparing for the 2026 World Cup¹³
- Verizon — F1 Miami Grand Prix 5G Private Network case study⁴
- Security Today — Hard Rock Stadium Verkada migration⁵
- VoltServer — Hard Rock Stadium DAS power case study¹
- Kele — BAS Behind the Game⁶
- ABB — Smart Stadium Automation⁷
- Wired — Inside Olympic Destroyer⁸
- Darknet Diaries Episode 77 — Olympic Destroyer⁹
- RSI Security — Cyber attacks at the 2018 PyeongChang Winter Olympics¹⁰

Sources & references

1. VoltServer's Digital Electricity platform at Hard Rock Stadium
<https://voltserver.com/blog/case-study/voltserver-powers-tech-at-hard-rock-stadium/>
2. multiple water systems are often included within cybersecurity planning scope
<https://www.nozominetworks.com/case-studies/protecting-the-2024-paris-olympics-critical-infrastructure-from-cyber-threats>
3. Reporting on recent event planning
<https://www.politico.com/news/2026/04/12/us-world-cup-cybersecurity-effort-hackers-threats-00860951>
4. Verizon 5G Private Network
<https://www.verizon.com/about/our-company/innovation-labs/case-study-f1>
5. unified Verkada cloud platform
<https://securitytoday.com/articles/2026/04/06/hard-rock-stadium-modernizes-security>



y-with-cloud-migration.aspx

6. Industry materials
<https://www.linkedin.com/pulse/bas-behind-game-systems-powering-modern-stadiums-kele-inc--xv3qe>
7. vendor documentation
<https://www.abb.com/global/en/company/stories/smart-stadium-automation>
8. coordinated disruption affecting IT systems
<https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/>
9. incident is often referenced
<https://darknetdiaries.com/transcript/77/>
10. downstream effects also reported at supporting venues
<https://blog.rsisecurity.com/cyber-attacks-at-the-2018-pyeongchang-winter-olympics/>
11. ANSSI and the Cyber Threat Alliance
<https://www.cyberthreatalliance.org/looking-beyond-the-medal-a-cybersecurity-after-action-report-on-the-paris-olympics/>
12. Public risk outlooks
<https://linden-nj.gov/fifa-world-cup-2026-cyber-threat-and-risk-outlook/>
13. reporting
<https://www.dataminr.com/resources/blog/preparing-for-the-2026-world-cup-security-challenges-and-how-to-tackle-them/>
14. CISA have publicly described ongoing engagement, exercises, and assessments
<https://www.whitehouse.gov/fifa-2026-task-force/>
15. a Region 4 tabletop exercise hosted by the City of Miami
<https://www.miami.gov/Notices/News-Notices/City-of-Miami-Hosts-Region-4-Miami-World-Cup-Tabletop%C2%A0Exercise>