



Home



My Network



Jobs



Messaging



Notifications



Me



For Business



Advertisement

[Edit article](#)

[View stats](#)

[View post](#)



From Border Gates to Stadium Seats: AI's Expanding Role in the World Cup and Olympics



John Binks, PMP®, AWS-CCP, AMA-CPM

Award-Winning / Best-Selling Author | Federal Growth & Business Development Executive | Federal Systems Integrator...



June 8, 2026

The upcoming FIFA World Cup and Olympics are not just sporting events.

They are global stress tests.

They will test airports, borders, stadiums, law enforcement, cyber defenses, transportation systems, media platforms, ticketing systems, public trust, and the ability of governments and industry to work together under pressure.

They will also test something else: our maturity with artificial intelligence.

The 2026 FIFA World Cup will be unlike any World Cup before it. It will be the first with 48 teams, three host countries, and 16 host cities across Canada, Mexico, and the United States. The 2028 Olympic and Paralympic Games in Los Angeles will bring another massive operational challenge, with hundreds of events, thousands of athletes, millions of fans, and a global audience watching in real time.

That scale matters.

A single stadium is hard enough to secure. A continental World Cup, followed by the Olympic Games, requires a system of systems. Airports, border crossings, hotels, transit hubs, training sites, fan zones, broadcast

operations, cloud platforms, mobile apps, payment systems, and social media ecosystems all become part of the event environment.

That is where AI becomes both powerful and complicated.

AI Is Moving from Novelty to Infrastructure

For years, AI in sports was often discussed through the lens of performance analytics, automated highlights, player tracking, and fan engagement.

Those uses still matter.

But the next chapter is bigger.

AI is now moving into the operational backbone of major events. It is being used to support identity verification, traveler screening, cyber defense, fraud detection, crowd management, threat intelligence, translation, venue operations, and public safety decision-making.

At the same time, robotics is becoming part of the visible security environment.

One recent example is Boston Dynamics' Spot robot. [Merry Frayne, Ph.D.](#) Senior Director of Product for Spot at [Boston Dynamics](#), did a great interview on CNN, discussing in the context of World Cup security. Spot is designed to move through spaces built for people, including stairs, uneven surfaces, and areas where fixed cameras may have limited visibility. In a security environment, robots like Spot can serve as mobile sensor platforms, helping security teams identify hazards such as abandoned bags, unsafe conditions, blocked pathways, and other issues that may require human attention.

That is an important distinction.

The robot is not replacing security professionals. It is extending their visibility.

Used properly, robotics can help people see around corners, inspect difficult areas, reduce unnecessary risk exposure, and send information back to a security operations center. The best model is not a robot-versus-human model. It is a robot plus a human.

That same principle should guide the broader use of AI.

The New Security Environment Is Bigger Than the Stadium

When most people think about event security, they picture the stadium entrance.

Metal detectors, Bag checks, Credential readers, Police presence, Cameras.

All of that still matters. But the modern threat surface is much wider.

The 2026 World Cup will span multiple countries, cities, agencies, jurisdictions, time zones, vendors, languages, and legal frameworks. The Olympics will bring similar complexity, with a dense concentration of venues, travel routes, hospitality zones, media operations, and digital platforms.

Security leaders should think in four connected layers.

1. The physical environment, including stadiums, fan zones, hotels, training sites, transit hubs, and public gathering spaces.
2. The digital environment, including ticketing, credentialing, payments, mobile apps, Wi Fi, broadcast systems, cloud services, and operational technology.
3. The information environment, including social media narratives, impersonation, misinformation, influence operations, deepfakes, online harassment, and panic amplification.
4. The human environment, including fans, athletes, families, workers, volunteers, officers, emergency responders, and local communities.

AI has a role in each layer.

But AI should not be treated as a magic fix placed on top of weak planning.

The best use of AI is not replacing planning. It is strengthening planning.

Biometrics, Borders, and the Fan Journey

For major events, identity verification and traveler processing are not side issues. They are core mission functions.

A World Cup or Olympics creates sudden surges of international travelers, credentialed workers, media, athletes, VIPs, vendors, volunteers, and emergency personnel.

AI-enabled biometric and digital identity systems can help speed processing and reduce friction at airports, borders, and controlled access points. They can also support anomaly detection, queue analysis, multilingual assistance, credential validation, and fraud detection.

But identity technology must be handled carefully.

Biometrics and facial comparison can improve speed and security, but they also raise real questions about accuracy, consent, data retention, oversight, redress, and public confidence.

Those questions cannot be treated as public relations problems. They are governance requirements.

People deserve to know what data is being collected, why it is being collected, how long it is retained, who has access, what happens when the system is wrong, and what alternative process exists for individuals who do not want to participate where alternatives are available.

Transparency is not the enemy of security.

It is a condition for trust.

Robotics Raises the Same Trust Question

Robots like Spot may be highly useful in venue environments, especially when used as mobile cameras or for remote inspection.

But they also raise concerns about public perception.

A robot walking through a crowded event will draw attention. Some people will find it impressive. Some will find it helpful. Some will find it unsettling.

That reaction is understandable.

The answer is not to dismiss public concern. The answer is to explain the purpose clearly.

In the Spot example, the robot is a tool used by people, with humans in the loop and security personnel reviewing the video feed. That is the right framing.

Robotics should be presented as an extension of human safety teams, not as an autonomous authority.

The public should not have to guess whether a robot is watching faces, scanning identities, or making enforcement decisions. Event organizers should state what the technology does and what it does not.

Clear communication matters.

Vague assurances do not.

On the Field, AI Is Already Changing the Game

AI will also be visible in match operations.

FIFA has already discussed AI-powered innovations for the 2026 World Cup, including analytics tools, 3D player avatars, referee-support technology, goal-line technology, semi-automated offside technology, and connected ball technology.

This shows one of the better patterns for AI adoption: narrow, defined use cases where technology assists human decision-makers.

That model should also guide security operations.

AI should support officers, analysts, emergency managers, transportation planners, medical teams, and cyber defenders. It should help them see patterns faster, prioritize resources better, and reduce noise.

It should not create an opaque operating environment where humans cannot explain why a decision was made.

The Cyber Threat Is Not Theoretical

Major sporting events are attractive targets because they combine money, attention, emotion, deadlines, and fragile dependencies.

Cybercriminals see ticketing platforms, fake travel sites, credential theft, payment fraud, ransomware, and phishing opportunities.

Hacktivists see symbolism.

State-aligned actors may see opportunities for espionage, disruption, or influence.

Fraudsters see fans who are excited, rushed, and willing to spend.

AI helps defenders, but it also helps attackers.

Defenders can use AI to detect abnormal login patterns, identify suspicious domains, triage suspicious communications, summarize threat intelligence, monitor credential exposure, and detect synthetic media.

Attackers can use AI to create more sophisticated phishing emails, clone voices, generate fake customer service messages, create convincing ticketing pages, produce synthetic images, and localize scams across languages.

That means every AI-enabled defensive strategy must assume an AI-enabled adversary.

The question is not whether AI will be used.

It already is.

The question is whether responsible organizations will use it with discipline, governance, transparency, and human accountability.

Digital Safety Is Now Event Safety

For the World Cup and Olympics, safety does not end at the stadium gate.

Athletes, officials, referees, teams, sponsors, and fans are also exposed online.

AI can help identify abusive, threatening, or discriminatory content at scale. FIFA and the International Olympic Committee have both used or discussed AI-supported approaches to reduce online abuse and protect athletes and officials.

This matters because online threats can become real-world risks.

A coordinated harassment campaign can affect an athlete's mental health. A deepfake can damage public trust. A fake emergency alert can create panic. A manipulated video can trigger confusion. A fraudulent ticketing site can steal money and personal information from thousands of fans.

Digital safety is no longer separate from physical safety.

It is part of the same operating picture.

The Leadership Challenge

The World Cup and Olympics will not be won by technology alone.

Disciplined planning, clear governance, strong partnerships, and human judgment will win them.

AI, biometrics, robotics, and digital identity tools can all improve major-event operations when deployed responsibly. They can help move people more safely, reduce friction, protect athletes, detect scams, support cyber teams, and give public safety leaders better visibility.

The lesson is simple: AI should make the human system stronger.

Not less accountable.

Recommendations for Leaders Preparing for the World Cup and Olympics

- Build an AI and robotics use-case inventory before the event begins.

Every agency, venue, contractor, and technology partner should know where AI, biometrics, video analytics, robotics, fraud detection, social media monitoring, translation, cyber defense, ticketing tools, and operational planning systems are being used.

If leaders cannot inventory the technology, they cannot govern it.

- Keep humans accountable for high-impact decisions.

AI can recommend, prioritize, flag, summarize, and accelerate. People must remain accountable for decisions that affect access, safety, rights, enforcement, and emergency response.

This is especially important for biometric, public-safety, robotics, and law-enforcement use cases.

- Treat robots as tools, not authorities.

Robots can extend visibility and reduce risk to personnel. They should not be presented as autonomous decision-makers. The public should understand what they do, what they collect, who reviews the information, and what limits apply.

- Red team the full digital fan journey.

Attackers will target emotional moments: ticket drops, hotel bookings, last-minute travel, mobile apps, VIP packages, parking, fake alerts, and streaming access.

Organizers should test the fan journey from search engine results to ticket purchase, airport arrival, transit, stadium entry, and post-event communications.

- Treat misinformation as an operational risk.

A fake evacuation notice, a deepfake official statement, a false security alert, or a manipulated video can have real-world consequences.

Event leaders should establish verified communication channels, rapid rumor-control processes, multilingual public messaging, and pre-approved escalation protocols.

- Protect athletes and officials online.

AI-enabled abuse detection should become standard practice for major events, paired with human review, platform coordination, mental health support, and clear reporting pathways.

- Modernize identity without losing public trust.

Biometrics and digital identity can reduce friction, but only when deployed with transparency, privacy controls, opt-out alternatives where applicable, clear retention rules, independent testing, and public explanation.

- Build a joint AI operations model.

Cyber, physical security, transportation, emergency management, public affairs, border processing, venue operations, and fraud teams should not operate from disconnected dashboards.

The value is not just the algorithm.

The value is the coordinated response.

- Require vendor accountability.

Major events depend on many vendors, including ticketing platforms, cloud providers, access control systems, analytics tools, camera systems, mobile app providers, robotics providers, hospitality partners, and payment processors.

Each should meet clear requirements for security, privacy, resilience, AI governance, incident reporting, and data handling.

- Communicate with the public like adults.

People understand that major events require security.

They also understand that technology can be misused.

Clear communication builds trust. Vague statements create suspicion.

The Leadership Lesson

AI will be one of the defining technologies behind the next era of global sports, alongside robotics, digital identity, and cyber intelligence. But none of these technologies replaces leadership. The strongest model is not AI everywhere. It is AI applied with purpose, where it clearly improves safety, fairness, resilience, and the overall experience, with humans remaining accountable for the outcome.

Billions of people will watch the World Cup and Olympics, but the real test will not simply be whether the games run smoothly. The deeper test will be whether we can use powerful technology in ways that are effective, explainable, secure, and worthy of public trust. That is the new standard for major events.

If you enjoyed this article, please share and repost.

Remember, the bots are getting smarter, but you're still the boss.

Copyright © 2026 John Binks / Bots & Bosses LLC, All Rights Reserved

#ArtificialIntelligence #AI #WorldCup2026 #FIFAWorldCup #Olympics
#LA28 #Robotics #BostonDynamics #Cybersecurity #HomelandSecurity
#Biometrics #DigitalIdentity #PublicSafety #SportsTechnology
#RiskManagement #ResponsibleAI #CriticalInfrastructure #EventSecurity
#FanExperience #JohnBinks #BotsAndBosses #BostonDynamics
#MerryFrayne

Comments



👤 2



Like

Comment

Share

Add a comment...



No comments, yet.

Be the first to comment.

[Start the conversation](#)



John Binks, PMP®, AWS-CCP, AMA-CPM

Award-Winning / Best-Selling Author | Federal Growth & Business Development Executive |
Federal Systems Integrator (FSI) | AI & Emerging Technology | Public Speaker / Podcaster |
Former FEMA Technology Executive

