ThreatRate
RISK MANAGEMENT



2026 FIFA WORLD CUP: RISKS AND THREAT ASSESSMENT

PUBLISHED
1 May 2026

CATEGORY
Other

OTHER · MAY 2026

2026 FIFA World Cup: Risks and Threat Assessment

Overview

The 2026 FIFA World Cup, scheduled from 11 June to 19 July 2026 across the United States, Mexico, and Canada, represents the largest tournament in FIFA history with 48 teams and 16 host cities. The event's geographic dispersion, extended duration, and unprecedented scale create a complex and multi-layered threat environment. Unlike previous tournaments concentrated in one country, the tri-national structure introduces cross-border vulnerabilities, uneven security capabilities, and logistical challenges. The tournament will generate dense concentrations of spectators not only inside stadiums but across fan zones, transport hubs, hospitality venues, and public gathering areas, significantly expanding the attack surface.

Key judgments

The most credible threat scenario is not a single mass-casualty attack but multiple smaller incidents across physical, cyber, and public-order domains. Soft targets outside stadiums – including fan zones, transport hubs, and nightlife areas – present the broadest exposure. Mexico carries the highest baseline crime and disruption risk, while the United States faces the broadest overall threat spectrum and Canada remains lower risk but not low consequence. Lone actors, protest-related disruption, cyber incidents, and localized criminal activity are the most plausible sources of operational impact.

Threat environment overview

The threat landscape is defined by a convergence of terrorism, organized crime, civil unrest, cyber threats, and opportunistic criminality. The most significant risk is not a single catastrophic event but a series of smaller, dispersed incidents capable of disrupting operations and shaping global perception. Soft targets such as fan festivals, public viewing areas, transportation systems, and nightlife districts remain the most vulnerable. The tournament's global visibility will attract a wide range of threat actors seeking symbolic, political, or financial impact.

Terrorism threat

The primary terrorism risk is driven by lone actors or small cells inspired by extremist ideologies rather than centrally directed plots. Individuals radicalized online or influenced by global conflicts can act with minimal preparation and low-complexity methods such as vehicle ramming, edged weapons, firearms, or improvised incendiary devices. The absence of a clear operational signature makes detection difficult and increases unpredictability.

A critical dimension of this threat is the risk posed by radicalized individuals with no clear affiliation to an established terrorist organization. These individuals often operate independently, do not communicate their intentions, and may not exhibit detectable links to known networks. As a result, they are particularly difficult to identify, monitor, or disrupt prior to an attack. Their lack of coordination and

© 2026 ThreatRate Risk Management. All Rights Reserved

minimal planning requirements allow them to exploit soft targets with little warning, making them one of the most challenging threat categories for security services during the tournament.

The ongoing conflict between the United States, Israel, and Iran has materially elevated the global terrorism threat environment in the lead-up to the 2026 FIFA World Cup. Although a temporary ceasefire is in place, it remains fragile, with core strategic issues unresolved and a high likelihood of renewed escalation. This instability sustains a heightened threat baseline rather than reducing it.

The conflict has intensified motivations for retaliatory and symbolic attacks against Western targets. Intelligence reporting indicates that Iran and Iran-aligned actors continue to pose a persistent threat to U.S. interests, including potential targeting of government entities, Jewish and Israeli-linked institutions, and dissidents on Western soil. This expands the threat spectrum beyond spontaneous lone actors to include state-linked operatives, proxy networks, and ideologically aligned individuals.

The war has also reinforced the role of proxy and affiliated groups such as Hezbollah and other Iran-backed networks, which retain the capability to conduct asymmetric attacks despite operational degradation. These groups, alongside affiliated or inspired individuals, may seek to exploit high-visibility international events to demonstrate continued relevance and retaliatory reach.

A key risk vector is the mobilization effect of the conflict across extremist ecosystems. The war has amplified anti-Western narratives, grievance-driven radicalization, and calls for retaliation, particularly in response to military strikes and civilian impact in the region. Historically, such conflicts correlate with spikes in both directed and self-initiated attacks, including by individuals with no formal organizational ties.

The threat is not limited to physical attacks. Iran has a well-documented capability in cyber operations and has previously signaled intent to target U.S. and allied infrastructure through both state actors and proxy hacktivist groups. In the context of the World Cup, this raises the risk of disruptive cyber activity targeting ticketing systems, transport infrastructure, media platforms, and critical services, potentially causing operational disruption and public panic.

Additionally, the conflict increases the likelihood of targeted or opportunistic attacks against specific communities and symbolic locations. Jewish, Israeli-associated, and diplomatic venues are assessed as higher-risk targets, particularly in cities hosting matches or large fan gatherings. There is also an elevated risk of violence linked to demonstrations, where geopolitical tensions may intersect with mass gatherings, creating opportunities for escalation or exploitation by hostile actors.

Importantly, the current environment reinforces the probability of low-complexity, high-impact attacks. The combination of heightened ideological motivation, global media attention, and accessible attack methods aligns with patterns observed in previous conflict-driven threat cycles. As a result, the most credible scenario remains a series of smaller-scale, decentralized incidents rather than a single coordinated attack.

Overall, the US/Israel–Iran war acts as a threat multiplier across all existing risk categories. It increases intent among a wider range of actors, expands the pool of potential perpetrators, and elevates both physical and cyber threat vectors. In the context of the 2026 FIFA World Cup, this dynamic further reinforces the vulnerability of soft

© 2026 ThreatRate Risk Management. All Rights Reserved

targets and the need for sustained, intelligence-led, and internationally coordinated security measures.



Potential targets linked to this dynamic include fan zones, large demonstrations related to the conflict, Jewish or Israeli-associated venues, diplomatic facilities, and crowded public areas. The risk is further heightened by the potential overlap between protest activity and extremist intent, where attackers may use demonstrations as cover or targets.

While the likelihood of complex, centrally directed attacks is lower, organized groups remain relevant as sources of propaganda,

© 2026 ThreatRate Risk Management. All Rights Reserved

inspiration, and remote facilitation. Terrorist organizations continue to encourage attacks in Western countries using simple, accessible methods. The strategic objective is less about operational sophistication and more about achieving psychological impact and global attention. Even a disrupted or unsuccessful plot could have significant consequences for public confidence and tournament operations.

Civil unrest and demonstrations

Civil unrest is expected to be a persistent feature throughout the tournament. The World Cup provides a global platform for activist groups seeking visibility for political, social, and ideological causes. Likely themes include the Middle East conflict, immigration, policing, climate change, economic inequality, and anti-globalization sentiment.

Most demonstrations will be peaceful; however, the scale of crowds, presence of opposing groups, and heightened security posture increase the risk of escalation. Flashpoints may include clashes between rival protest groups, confrontations with law enforcement, and attempts to disrupt matches or access restricted areas. Demonstrations could also target sponsors, government institutions, or symbolic locations associated with participating nations.

There is a credible risk that extremist actors may exploit these gatherings, either by targeting them directly or using them as operational cover. The intersection of protest activity and terrorism risk requires integrated public order and counterterrorism planning.

Crime and public safety

Crime will be widespread and, in many cases, more likely than terrorism to affect visitors. Common risks include pickpocketing, robbery, scams, ticket fraud, and assault, particularly in crowded areas and nightlife districts. High visitor volumes, unfamiliar environments, and visible affluence increase vulnerability. In the United States and Canada, crime risks are generally manageable but will increase in host city centers during peak periods. In Mexico, the risk profile is significantly higher due to the presence of organized criminal groups and elevated levels of violent crime.

Cyber threats

Cyber threats represent a critical and often underestimated risk. State and non-state actors have the capability to disrupt digital infrastructure associated with the tournament. Potential targets include ticketing systems, accreditation platforms, transportation networks, stadium operations, and financial transactions.

Cyberattacks could result in operational disruption, denial of access, data breaches, or widespread confusion. Disinformation campaigns, including false security alerts or manipulated content, could trigger panic or undermine public confidence. Given the geopolitical environment, cyber activity linked to state actors or ideologically motivated groups is a credible concern.

Host country comparison

© 2026 ThreatRate Risk Management. All Rights Reserved

Mexico



Mexico presents the most complex security environment among the host nations. Organized crime groups, particularly drug cartels, maintain significant operational capacity and territorial influence. These groups are not expected to deliberately target the World Cup; however, their activities pose a substantial indirect risk.

The reported killing of Jalisco New Generation Cartel leader Nemesio Rubén Oseguera Cervantes, known as El Mencho, in Tapalpa, Jalisco, has triggered a period of instability and potential fragmentation within the organization. Such developments historically lead to retaliatory violence, power struggles, and demonstrations of force. These can include road blockades, vehicle burnings, attacks on infrastructure, and disruptions to transportation networks.

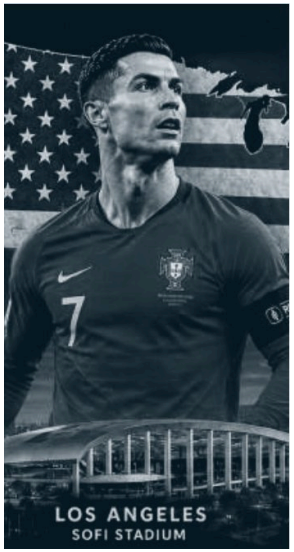
Guadalajara, located in Jalisco and a host city, is particularly exposed. The city lies within a region of strong cartel influence, and previous incidents have shown the capacity for rapid, large-scale disruption affecting urban mobility and public safety. Even without direct targeting of World Cup venues, cartel-related actions could impede access routes, disrupt logistics, and create localized insecurity.

Monterrey and Mexico City face different but still significant risks. Monterrey is a major industrial hub with exposure to organized crime activity and potential spillover violence. Mexico City, as the capital, combines high crime rates with a strong likelihood of large-scale demonstrations and symbolic targeting. Across all Mexican host cities, risks include kidnapping, extortion, armed robbery, and collateral exposure to violence.

For most visitors in Mexico, the most likely threat is opportunistic crime rather than direct cartel targeting. The principal risks are robbery, theft, scams, and transport-related crime, with express kidnapping remaining a relevant but less common concern, particularly for higher-profile or affluent travelers. Risk is not uniform across host cities, Mexico City, Guadalajara, and Monterrey are expected to see a strong security presence during matches, but exposure increases at night, outside main tourist zones, and when using informal or unregulated transport.

© 2026 ThreatRate Risk Management. All Rights Reserved

United States



The United States faces the broadest threat spectrum because of the number of host cities, the scale of operations, and the complexity of coordinating security across multiple jurisdictions. The primary concerns are lone-actor terrorism, protest-related disruption, cyber incidents, and opportunistic crime in dense urban environments. These risks are mitigated by mature federal, state, and local security capabilities, strong intelligence-sharing mechanisms, and extensive experience securing major events, which should keep overall risk manageable for most visitors.

Canada



Canada presents the lowest baseline risk among the three hosts but remains exposed to lone-actor threats, cyber disruption, and protest activity in major urban centers. Its comparatively favorable security environment reduces the likelihood of high-volume criminality, but high-visibility venues and public gathering areas will still require strong protective measures. The principal challenge is not persistent violence but the potential for a lower-frequency incident to have outsized operational or symbolic impact.

Key risk scenarios

The most plausible scenarios include a lone-actor attack targeting a fan zone or public gathering area, violence occurring in or around demonstrations linked to the Middle East conflict, cyber disruption affecting ticketing or stadium access systems, cartel-related road

© 2026 ThreatRate Risk Management. All Rights Reserved

blockades or infrastructure attacks in western Mexico, and widespread petty or violent crime incidents affecting visitors.

Conclusion

The 2026 FIFA World Cup will take place in a highly dynamic and complex global security environment. The convergence of geopolitical tensions, particularly the war in the Middle East, evolving terrorism trends, organized crime in Mexico, and the inherent vulnerabilities of mass gatherings creates a multi-dimensional threat landscape.

The most significant risk is not a single large-scale attack but a combination of smaller incidents across multiple domains that collectively disrupt operations and erode public confidence. Effective mitigation will depend on coordinated cross-border security efforts, intelligence sharing, robust public order management, cyber resilience, and targeted risk awareness for participants and spectators.

© 2026 ThreatRate Risk Management. All Rights Reserved



Risk intelligence that keeps you safe

ABOUT THREATRATE

ThreatRate helps you benchmark your risk management strategy against rapidly evolving global and local trends, with real-time, actionable analytics and insights.

For more information contact us at

info@threatrate.com

MEMBERS HAVE ACCESS TO

100+
risk-focused reports published annually

API
customised access option

Dashboards
customised dashboards and infographics

Experts
ThreatRate analysts with cross-industry depth

© 2026 ThreatRate Risk Management. All Rights Reserved

ThreatRate RISK MANAGEMENT