CYBER THREAT ANALYSIS

Recorded Future®

Insikt Group®

June 4, 2026

Threats to the 2026 FIFA World Cup

Mexico's host cities face the highest physical risk from organized crime, while US venues face limited but real threats to soft targets like fan zones, watch parties, and transit hubs.

Cybercriminals are already exploiting World Cup branding through fake FIFA stores, purchase scams, and phishing, while AI-generated content is set to accelerate fraud at an unprecedented scale.

Influence operations from Russia, China, and Iran remain overwhelmingly overt through state media and diplomatic channels; covert operations remain limited despite their agile, opportunistic nature.

Executive Summary

The 2026 FIFA World Cup, which takes place across sixteen host cities in the United States (US), Mexico, and Canada, presents a complex threat environment across multiple security domains. The tournament's global visibility creates opportunities for both financially and geopolitically motivated threat actors to target attendees, affiliated organizations, sponsors, vendors, and event-supporting infrastructure.

Physical security will almost certainly remain the highest priority for event coordinators and local government officials, given the high levels of international attention and the concentration of large crowds in host cities spanning three countries and multiple, distinct security environments. Mexico's host cities face the highest physical risk due to the persistent presence of local and transnational criminal organizations (TCOs), with elevated concerns around theft, extortion, kidnapping, and fraud. US and Canadian host cities likely face a more limited threat from violent extremists, with greater risks to soft targets such as fan zones, watch parties, transit hubs, and other crowded public areas.

Civil unrest and disruptive protests are also very likely in a majority of host cities. Localized travel disruptions are especially likely in Mexico, where prior demonstrations have already blocked roads near World Cup venues. Large police or military deployments near event sites will likely increase the risk of confrontation.

The most immediate risk to corporate sponsors and affiliates is likely cybercriminal exploitation of World Cup demand and branding. Recorded Future's Payment Fraud Intelligence team has already identified World Cup-themed purchase scams, fake FIFA-branded stores, and spoofed FIFA and host city domains. Carders are also likely to leverage stolen payment card credentials to fraudulently purchase event tickets and travel-related services for rapid resale and monetization. Efforts to use individuals' interest in the World Cup to deliver malware or carry out data extortion or fraud will likely accelerate as the tournament approaches. Threat actors will likely continue to use AI-generated content to scale fraud, impersonation, phishing, smishing, and social engineering campaigns.

The concentration of senior government officials, diplomats, security personnel, corporate executives, and media at World Cup events also very likely increases the risk of cyber espionage and disruptive cyber incidents. Russian, Chinese, and Iranian state-sponsored threat groups will likely use the tournament as an intelligence collection opportunity, targeting executives, VIP attendees, national delegations, media partners, telecommunications providers, airlines, hotels, event logistics firms, and commercial affiliates. China is most likely to pursue targeted espionage, while Russia and Iran pose a higher risk of more disruptive attacks through proxy hacktivism.

Influence activity related to the tournament remains largely overt, driven by state media and diplomatic messaging from Russia, China, and Iran. These narratives focus on host-country legitimacy, Iran's conditional participation, visa and access issues, public safety, immigration, ticketing, and alleged politicization of the event. Covert influence activity has so far been limited and opportunistic, but could

increase as the tournament approaches, particularly around geopolitical flashpoints or viral news events.

Organizations involved in or exposed to the World Cup should prioritize proactive monitoring of location-specific physical security risks, protest activity, cybercriminal infrastructure, phishing and credential exposure, malicious traffic, ransomware indicators, and influence operations. Cyber indicators such as increased scanning activity or newly registered domains linked to FIFA or host cities may indicate an expansion of criminal or espionage activity. Developments around geopolitical flashpoints such as the Iran War may increase the likelihood of attempts to disrupt the tournament through cyber or physical attacks.

Key Findings

- World Cup crowds will likely elevate physical security risks around match venues and fan areas, exacerbated by factors such as TCO activity in Mexico and impending primary elections and 250th Independence Day celebrations in the US.
- Opportunistic criminal activities tied to organized crime very likely constitute the largest physical security risks to Mexico's World Cup host cities, while US venues face very likely less substantial (but nonetheless tangible) threats from violent extremists, particularly homegrown violent extremists (HVEs).
- Cybercriminal threat actors are exploiting World Cup-themed branding via purchase scams and phishing infrastructures, with AI-generated content likely enabling operations to surpass volumes observed during prior World Cups. Carders frequently use fraudulent ticket purchases and resale schemes as a rapid monetization method for stolen payment card credentials.
- Russian, Chinese, and Iranian state-sponsored threat groups will likely use the World Cup as an intelligence collection opportunity, while Russia and Iran pose additional risks of disruptive cyber operations, particularly from proxies and hacktivist personas.
- World Cup-related influence activity from Russia, China, and Iran is driven overwhelmingly through overt state media and diplomatic messaging, while observed covert activity remains limited, opportunistic, and largely secondary to broader geopolitical narratives about Iran, host-country legitimacy, and US access and security policies.

Table of Contents

Country Risk

Insikt Group assessed four categories of country-level risk in World Cup host countries: security and crime data; network intrusion activity, which measures Malicious Traffic Analysis events targeting each country; ransomware attacks targeting victims in each country; and data privacy and surveillance-related risks, accessible in the Recorded Future Intelligence Operations Platform as State Surveillance risk. While public reporting indicates declining crime rates in many World Cup host cities, violent crime risks are almost certainly greatest in Mexico; opportunistic crime, such as theft, likely presents the greatest physical security risk in Canadian and US host cities. By comparison, threats to data security and privacy are likely greatest in the US and Canada, given the higher volume of malicious cyber activity targeting US and Canadian entities. Factors complicating the security environment across World Cup host nations include TCO operations in Mexico; 250th anniversary celebrations in the US; and the lead-up to the US midterm elections in November 2026, including summer primary elections.

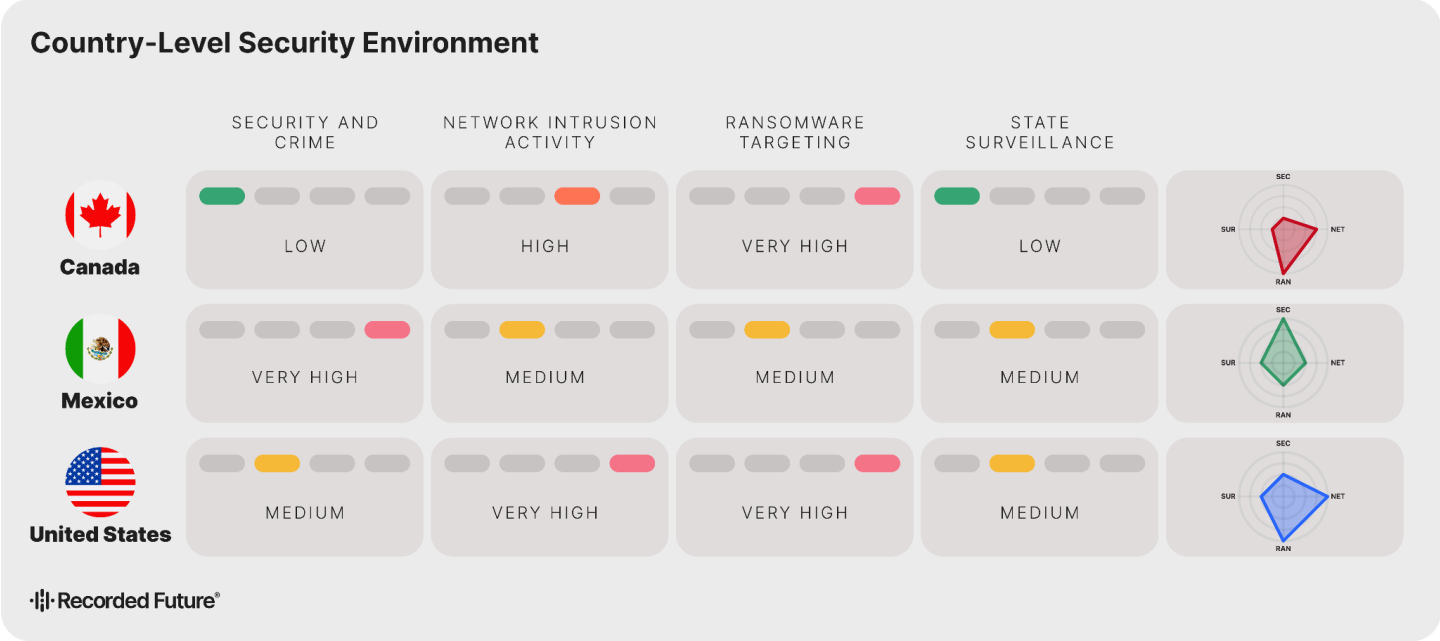


Figure 1: *Composite Country Risk Scores for Canada, Mexico, and the US (Source: Recorded Future)*

Canada

Political and Security Landscape

The physical threat level in Canada is likely low, with opportunistic petty crime in crowded areas likely presenting the primary threat to travelers. The US Department of State currently advises exercising normal precautions in Canada, noting that destinations in Canada are generally safe for travelers. The Department of State's Overseas Security Advisory Council (OSAC) specifically designates most major cities in Canada, including host cities Toronto and Vancouver, as low-threat locations for crime, terrorism, and political violence. Since October 2014, Canada's National Terrorism Threat Level has

remained at medium, the third level of its five-level threat scale. This level indicates that a violent act of terrorism "could occur," but falls short of assessing that an attack is likely.

Digital Threat Landscape

Based on analysis of malicious traffic over the first quarter of 2026, Insikt Group assesses that the network intrusion activity risk in Canada is high, reflecting a high volume of observed suspicious and malicious behavior, based on evidence of hosts communicating over a known command-and-control (C2) channel. Insikt Group assesses that the threat from ransomware to Canada-based entities is very high, with 110 attacks targeting Canadian organizations in the first quarter of 2026, accounting for approximately 5% of ransomware attacks globally observed by Recorded Future during that period. This aligns with the Canadian Centre for Cyber Security's 2025–2026 National Cyber Threat Assessment, which identified ransomware as "the top cybercrime threat facing Canada's critical infrastructure."

Insikt Group assesses that digital surveillance in Canada poses a low threat to privacy and the security of data transmission. While the Canadian government almost certainly possesses advanced digital surveillance capabilities, these are exercised under a comprehensive system of oversight and judicial review. In March 2025, The Citizen Lab reported "a growing ecosystem of spyware capability" among Ontario police services, after identifying server infrastructure that indicated potential use of Paragon Solutions' Graphite spyware by the Ontario Provincial Police. Toronto and Vancouver police have expanded surveillance architecture ahead of World Cup matches to facilitate real-time monitoring of crowd movements and public safety threats, including the temporary installation of surveillance cameras in fan zones and high-traffic areas. However, Insikt Group has not identified evidence of unlawful surveillance, indicating that surveillance and data privacy-related risks for foreign travelers likely remain low.

Host City Security Environment

Opportunistic petty theft likely remains the predominant security threat to tourists traveling to World Cup events in Canadian host cities, though both national and local crime data indicate declining incidents of violent and non-violent crime. Canada's Crime Severity Index (CSI), which measures the volume and severity of police-reported crime in the country, decreased 4% in 2024 following three years of increases, according to the latest data published in July 2025. While the decline was primarily driven by decreases in non-violent crimes, the CSI also recorded declines in attempted murder (-12%), aggravated assault (-8%), sexual assault (-3%), and robbery (-2%).

According to Vancouver Police Department (VPD) crime statistics as of May 2026, homicides and violent crime (categorized as offenses against a person) have both fallen in the last year. VPD reported three homicides in the last eight weeks, representing an 80% decline from the same period in 2025, and 429 violent crimes, a 15% decline. Since early 2026, one homicide and 275 incidents of violent crime have occurred within 1,000 meters of BC Place in Vancouver, which will host World Cup matches. Similarly, the Toronto Police Service (TPS) reports 47 assaults, burglaries, robberies, and thefts since early 2026 in the Fort York-Liberty neighborhood, where Toronto's BMO Stadium will host World Cup

matches. This represents a 25% decrease from the same period in 2025. TPS reports no homicides in the Fort York-Liberty neighborhood in 2026, compared to one in 2025.

Mexico

Political and Security Landscape

Mexico's physical security environment, which varies significantly by state and municipality, sees persistent physical security threats in the form of violent crimes such as kidnapping, extortion, carjacking, robbery, and organized crime-related violence. The US Department of State currently advises increased caution in Mexico, with some states subject to warnings against travel, and warns that organized crime groups remain active across multiple states. OSAC lists Mexico City as a critical-threat location and Guadalajara and Monterrey as high-threat locations for crime; it lists Mexico City and Guadalajara as high-threat locations and Monterrey as a medium-threat location for political violence. Areas along the northern border region, parts of the Pacific coast, and states with entrenched drug trafficking organization presence represent elevated risks, while major urban and tourist areas generally have stronger security infrastructure. Even these areas, however, see relatively high rates of theft, armed robbery, express kidnapping, and violence. In February 2026, the US Embassy in Mexico issued a security alert for roadblocks and criminal activity in Jalisco, home to the host city of Guadalajara, following a high-profile operation against a major organized crime group in the area (see "Physical Security" section below).

Digital Threat Landscape

Based on analysis of malicious traffic over the first quarter of 2026, Insikt Group assesses that the network intrusion activity risk in Mexico is medium, reflecting a moderate volume of observed suspicious and malicious behavior based on evidence of hosts communicating over a known C2 channel. Insikt Group assesses the ransomware threat to Mexico-based entities as medium, with 22 attacks targeting Mexican organizations in the first quarter of 2026, or approximately 1% of ransomware attacks globally observed by Recorded Future during that period.

Insikt Group assesses that digital surveillance in Mexico poses a moderate threat to privacy and the security of data transmission. Analysts did not identify any evidence of unlawful domestic surveillance under the current President, Claudia Sheinbaum, but Mexican intelligence, law enforcement, and military forces used commercial spyware — most notably NSO Group's Pegasus spyware, as well as spyware from Circles and QuaDream — during successive previous administrations, including to target government critics and journalists. In February 2024, R3D reported that the Cyberspace Operations Center under the Secretariat of National Defense had used HIWIRE monitoring software from Israeli firm WebintPro to identify links between social media users critical of the Mexican Armed Forces or the government as recently as May 2022. Further, in 2020, Forbidden Stories reported that police had helped some cartels obtain access to commercial spyware typically marketed only to government actors, citing an unnamed senior Drug Enforcement Agency official.

Host City Security Environment

Inter-TCO violence and territorial disputes in and around host cities in Mexico will likely elevate baseline security risks during the tournament period, even if not directly linked to World Cup events. At the same time, official statistics indicate that criminal violence in Mexico has fallen in recent months. According to the Executive Secretariat of the National Public Security System, the daily national average of intentional homicides has fallen by roughly 40% from when President Claudia Sheinbaum took office in October 2024 to April 30, 2026, declining from 86.9 to 52.5 homicides per day.

Official crime statistics for Mexico City, the state of Jalisco, and the state of Nuevo León — each of which will host World Cup matches — also show significant reductions in homicides compared to the previous year. In March 2026, the Guadalajaran government reported that "high-impact" crimes — homicide, robbery, and theft — had fallen by 25% year-over-year, based on a comparison of data from the first two months of 2026 and 2025. Homicides fell by 15%, from 28 in the first two months of 2025 to 24 in 2026. Nuevo León state authorities claimed that homicides in the state hit a fifteen-year low in April 2026, with "very considerable reductions" in the city of Monterrey and the municipality of Apodaca, and zero homicides in several municipalities of the Metropolitan Monterrey area. Governor Samuel García claimed that the number of homicides in the state had declined by 63% compared to 2025. Similarly, the Mexico City government claimed that "high-impact crimes" had fallen by 7% since 2025, with homicides recorded from January to April 2026 representing the lowest number in that period since 2022.

United States

Political and Security Landscape

Physical security threats in the US vary across cities; violent crime occurs more frequently in major cities, and opportunistic crime, such as theft, likely presents the greatest threat to World Cup travelers. These risks are very likely greatest in the most densely populated host cities — namely, New York City, Los Angeles, and Miami — in crowded public spaces, such as public transit, tourist attractions, or World Cup fan zones. On May 7, US Department of Homeland Security Secretary Markwayne Mullin stated that security threats were particularly high "in soft areas outside of the stadiums." The Canadian government currently advises travelers to the US to take normal security precautions, noting that petty crime is most common in urban centers and tourist areas.

World Cup matches will occur in the lead-up to the US midterm elections in November 2026, with primary elections in many states between June and August. Politically motivated protests in major US cities remain possible around primary election dates, though such activity will likely increase in frequency closer to November. While none of the World Cup matches coincide directly with primaries in their respective host cities, the upcoming Norway-Senegal match on June 22, held at New York City's MetLife Stadium, will take place one day before the New York state primary elections on June 23.

Digital Threat Landscape

Based on analysis of malicious traffic over the first quarter of 2026, Insikt Group assesses that the network intrusion activity risk in the US is very high, with the US consistently experiencing the highest volume of observed suspicious and malicious behavior based on evidence of hosts communicating over a known C2 channel. Similarly, the threat from ransomware to US-based entities is very high, with 1,176 attacks targeting US organizations in the first quarter of 2026 — approximately 50% of the ransomware attacks globally observed by Recorded Future during that period. The Office of the Director of National Intelligence (ODNI) Annual Threat Assessment identified ransomware attacks as particularly harmful to US critical infrastructure and business operations, assessing that ransomware groups were shifting to "faster, high-volume attacks" that complicate identification and mitigation efforts.

Insikt Group assesses that digital surveillance in the US poses a moderate threat to privacy and the security of data transmission, based on the US's advanced digital surveillance capabilities and recent expansions of surveillance for immigration purposes, which have likely increased surveillance-related risks for foreign nationals and near-border zones. In June 2025, the US Department of State instructed all applicants for F, M, and J nonimmigrant visas to set privacy settings on their social media profiles to public — facilitating monitoring of the social media activity of a broad range of foreign nationals seeking to enter the US. In the same month, reports emerged that the US Immigration and Customs Enforcement Agency (ICE) was using a new mobile application with facial recognition, dubbed "Mobile Fortify," to identify individuals in real time using smartphone cameras, with "contactless fingerprints and facial images captured" and compared to biometric data collected at points of entry to the US. Citing immigration-related surveillance measures, in April 2026, over 120 civil society groups issued an advisory stating that there is an increased likelihood of social media screening and electronic device searches targeting travelers to the US. The US government's search-and-seizure authorities, while generally limited by the US Constitution's Fourth Amendment, are already significantly broadened in "border zones," defined as up to 100 miles from any US border.

Host City Security Environment

According to preliminary 2025 crime data released by the Federal Bureau of Investigation (FBI) in April 2026, the US experienced a 9.3% decrease in violent crime and a 12.4% decrease in property crime. Based on local police department data as of March 2026 (**Appendix A**), rates of violent crime and theft significantly surpass the national average in most US host cities, but have largely declined since 2025. Theft very likely remains the most prevalent security concern for travelers attending World Cup events in most US host cities.

Several US World Cup matches will coincide with Independence Day weekend celebrations, including July 3 matches in Dallas and Kansas City; July 4 matches in Houston and Philadelphia, and the July 5 match in New York City. In addition to very likely presenting high-value targets for low-level criminal activity, the convergence of World Cup matches and 250th Independence Day festivities will almost certainly be accompanied by stricter security measures and restrictions in public spaces, as US

security agencies have historically warned of an increased risk of violence targeting July 4th festivities. In June 2025, the FBI and Department of Homeland Security (DHS) issued a joint bulletin warning that attacks perpetrated by lone offenders or small groups represented the biggest terrorism threat to July 4 celebrations in New York City and elsewhere.

Physical Security

Mexico's World Cup host cities — Guadalajara, Mexico City, and Monterrey — will very likely face the highest levels of physical risk during the 2026 FIFA World Cup. Threat actors associated with Mexico-based local and transnational criminal organizations (TCOs) are very likely to increase opportunistic physical threat activities in World Cup host cities, thereby increasing the risk of crime and violence targeting attendees and disruptions to inter- and intra-city transportation corridors. At present, Insikt Group has not identified significant evidence of terrorist or violent extremist threats to the 2026 FIFA World Cup, although soft targets in major US metropolitan areas currently face heightened risks from violent extremist physical threat activities.

Organized Crime

TCOs based in Mexico, along with local criminal structures, will very likely pose a persistent physical security threat to 2026 FIFA World Cup–related activities, particularly in the three host cities in Mexico and along key transit corridors. While these groups are unlikely to deliberately target official match venues due to the high security presence and the risk of provoking an overwhelming government response, they will likely seek to exploit the influx of international visitors, elevated economic activity, and strained local security resources in order to advance illicit economic interests and demonstrate local control. TCO-linked and local criminal actors will likely increase opportunistic criminal activity, including theft, express kidnapping, extortion, and fraud schemes targeting tourists, hospitality operators, and transportation providers. Additionally, criminal groups may attempt to infiltrate or co-opt local supply chains supporting the tournament — such as food, merchandise, and transportation — to benefit from tournament-related revenue or expand their group's influence.

Recent high-profile violent incidents (primarily shootouts with security forces and roadblocks) in Guadalajara, Jalisco, following the February 22, 2026, Mexican military operation that killed Nemesio Rubén Oseguera Cervantes, alias "El Mencho," former head of the Jalisco New Generation Cartel (Cártel de Jalisco Nueva Generación; CJNG), underscore the elevated risk of TCO-linked violence around the tournament. Although the homicide rate in Jalisco has fallen in recent years and Insikt Group has assessed that CJNG leadership cohesion means the organization is less likely to disrupt the World Cup through high-profile displays of violence, the possibility cannot be ruled out. The CJNG and other TCOs in Mexico have historically demonstrated the capability to conduct large-scale disruptive acts — such as road blockades, arson attacks, and coordinated armed confrontations — that could disrupt mobility and logistics during the event. Although such actions are typically directed at rival TCOs or security forces, their occurrence during the World Cup would almost certainly have significant secondary impacts on public safety and event operations.

Terrorism and Violent Extremism

US-based violent extremists are likely to plot attacks targeting 2026 FIFA World Cup events in the US, but the physical security footprint surrounding the games will very likely reduce the likelihood of a successful attack or mitigate the impact. At the time of writing, Insikt Group has not identified communications from homegrown violent extremists (HVEs), domestic violent extremists (DVEs), or foreign terrorist organizations (FTOs) indicating threats to the World Cup.[1] Nevertheless, the US currently faces heightened risks of violent extremist physical threat activity. Violent extremist attacks targeting the World Cup are less likely to directly target event venues and more likely to target their audiences, related events, and supporting infrastructure — including high-profile public figures attending the events, "fan zones" and watch parties, nearby transportation infrastructure, and lodging and hospitality facilities for fans.

The most likely violent extremist threat actors to plan attacks targeting the World Cup are HVE supporters of the Islamic State (IS). Unlike other categories of violent extremists, IS supporters in the US have demonstrated both the intent and the capabilities to attack targets related to sporting events in recent years. The most recent incident of this type was the January 1, 2025, attack in New Orleans on the day of the 2025 Sugar Bowl, which killed fourteen. Throughout 2024, IS official media outlets and supporters frequently incited or threatened terrorist attacks at European sporting venues; police in France disrupted several IS-linked attack plots in the months prior to the 2024 Paris Olympics.

It is plausible that other categories of violent extremist threat actors — including HVE supporters of Iran or its "axis of resistance" groups, and DVEs of various ideological persuasions — could conduct physical threat activities targeting the World Cup. Iran-nexus physical threat actors in the US, in particular, have almost certainly increased operations following US strikes on Iran in the summer of 2025, coinciding with a spate of DVE attempted attacks and threats targeting US government officials. At present, however, Insikt Group has not identified evidence that these threat actors intend to conduct attacks targeting the World Cup, nor that they have attacked targets connected to large-scale sporting events or venues in the last five years.

Civil Unrest and Disruptive Protests

Protests, demonstrations, and strikes coinciding with World Cup events will very likely take place in a majority of host cities. To date, Insikt Group has identified anti-World Cup demonstrations in Los Angeles, Toronto, Vancouver, Guadalajara, Mexico City, and Monterrey that have already occurred or are scheduled to coincide with the World Cup.

The risk of protests disrupting events, travel, or infrastructure is almost certainly contingent on the host city and country. Demonstrations in Mexico — including anti-FIFA and anti-World Cup protests and strikes by labor activists, the families of "desaparecidos" (missing people), and anti-gentrification

[1] Insikt Group uses definitions of terrorism and violent extremism adapted from US Intelligence Community (IC) definitions, academic research, and open-source reporting.

groups — are especially likely to cause local travel disruptions. On March 28, 2026, a group protesting what it called "The World Cup of Dispossession" blockaded a section of the Anillo Periférico Sur highway near Mexico City's Banorte Stadium, during a Mexico-Portugal friendly match (**Figure 2**). The Mexican government has reportedly mobilized over 100,000 law enforcement and military personnel to ensure security at World Cup sites (the strategy is known as "Plan Kukulkán"), increasing the likelihood of violent confrontations between demonstrators and police.

Figure 2: *Protestors occupy and blockade a section of highway near Mexico City's Banorte Stadium (Source: Reuters)*

State-Sponsored Cyber Threats

Iran

Iranian state-sponsored groups are likely to conduct disruptive attacks against the World Cup. Both Iran's Ministry of Intelligence and Security (MOIS) and Islamic Revolutionary Guard Corps (IRGC) have previously leveraged hacktivist personas to conduct deniable disruptive operations in response to geopolitical events. IRGC-linked hacktivist personas have been known to target sporting events, and open-source reporting suggests Iran has the intent to carry out physical attacks during the World Cup. This intent may drive the risk of increased disruptive or destructive cyber operations during the event.

Given the current conflict, Iran likely views US organizations as legitimate targets for disruptive and likely also destructive cyberattacks. Iran's hacktivist personas may be used to amplify the effects of a range of activities, from low-level DDoS and web defacement to hack-and-leak activities, ransomware, or wiper deployment.

Disruption

In the wake of Operation Epic Fury, the Trump administration has questioned Iran's participation in the World Cup. Iranian Football Federation personnel have also been denied official entry into Canada and were not able to attend the April 2026 FIFA Congress, specifically due to their reported affiliations with the IRGC. This has led to tensions between FIFA's leadership and representatives of the Iranian Football Federation and, subsequently, the Iranian government. At least three known groups retain the capabilities and historical predisposition to target networks directly related to FIFA or those supporting it; they include Handala Hack Team, GreenHotel (Ayandeh Sazan Sepehr Aria, Cotton Sandstorm, Emennet Pasargad), and GreenBravo (APT42, Charming Kitten, Mint Sandstorm, TAG-83). Iran may also use existing assets or create new hacktivist personas, such as Ababil of Minab, that are specifically focused on targeting the World Cup.

Handala Hack Team

Handala Hack Team has been attributed to Void Manticore (TAG-145, Red Sandstorm, Banished Kitten), a threat cluster linked by the US Department of Justice to Iran's MOIS. The group is one of several personas used by MOIS to target Israel, Iranian opposition groups, and increasingly US entities.

Handala Hack Team has achieved high global visibility due to its role in Iran's asymmetric retaliation campaign against the US and Israel, as well as extensive media coverage since the start of operations Epic Fury and Roaring Lion. Since the onset of the conflict on February 28, 2026, the group has increased its claimed cyber operations against US targets, including Stryker, county government infrastructure, FBI Director Kash Patel, and US Marine Corps personnel. In Handala's claim of responsibility for targeting Stryker, the group stated it was an act of retribution for the Minab school bombing.

Insikt Group has not identified information suggesting that Handala is planning to target networks associated with the FIFA World Cup; however, as of this writing, it retains the capabilities and intent to target US private and public networks. The group also uses its operations as part of its influence activity against the US, and is therefore likely in a position to inflict reputational damage on FIFA, the US administration, and various sectors that will service the tournament.

GreenHotel

GreenHotel has an established history of executing hybrid operations targeting sporting, media, and event-related organizations, including targeting Israeli athletes. The group's objectives combine intelligence collection with influence operations and disruptive capabilities. US government agencies also highlighted the group's expanded operational remit, which led to the targeting of at least one US media organization, IPTV, by "For Humanity", a suspected GreenHotel persona.

In 2024, Insikt Group reported on Zeus Hacking Group, an Iranian hacktivist persona likely managed by GreenHotel. The persona was used to target Israeli Olympic athletes, in addition to the National Sports Center of Israel, and subsequently led a doxxing campaign during the 2024 Paris Olympic Games. While no information has been identified to suggest that GreenHotel is targeting athletes attending the World Cup, the Zeus campaign demonstrates the group's intent to specifically target sporting personnel for political and ideological motives.

Figure 3: *Zeus established multiple social media profiles to amplify the spread of its message and doxxing attacks on athletes representing Israel (Source: Recorded Future)*

GreenBravo

GreenBravo (APT42) remains a key component of Iran's cyber and influence apparatus. The group has conducted intrusion activity and leveraged stolen material in support of broader influence operations

intended to influence the 2024 US election cycle and exacerbate sociopolitical tensions within targeted audiences. Throughout 2024, APT42 operated the pro-Iranian online persona "Robert," which US officials publicly linked to the IRGC.

The group disseminated material reportedly exfiltrated from President Donald Trump's campaign, indicating that Tehran's election interference activity remained ongoing through at least late 2024. In September 2024, a "Robert" persona circulated a campaign-related document to journalists, reinforcing concerns that Iranian threat actors retained access to sensitive campaign communications. Microsoft and Google separately attributed the activity to APT42, assessing that the group targeted high-profile individuals affiliated with both the Trump and Biden campaigns, as well as government and policy personnel. The activity mirrored operational patterns previously observed during the 2020 US election cycle. Although multiple intrusion attempts were reportedly disrupted, at least one senior consultant's Gmail account was successfully compromised.

Although Insikt Group has not identified credible reporting indicating imminent targeting of the US administration or US officials associated with the 2026 FIFA World Cup, the likelihood of attempted intrusion or influence operations conducted by APT42 remains elevated.

Ababil of Minab

As discussed in the **Malign Influence Operations** section below, Iran's football team will be named "Minab-168", referencing the bombing of a school in Iran at the onset of the Iran War in February 2026. In April 2026, Insikt Group reported on a new hacktivist persona, "Ababil of Minab", which claimed disruptive attacks against multiple US-based organizations and is likely operated by Iran state-sponsored threat actors (tracked as ION-87 by Insikt Group). This persona may be leveraged to target the upcoming World Cup.

Espionage and Surveillance

Iran's espionage and surveillance groups remain a persistent threat to the World Cup due to the increased politicization of the Iran War, anti-government leadership (Shah Reza Pahlavi), and human rights advocates present in the US. Key groups responsible for espionage activity, with a possible remit to lead operations during the tournament, include GreenBravo, GreenCharlie, GreenGolf, GreenEcho, and TAG-182. Common malware and phishing capabilities deployed by these groups to target victims include TAMECAT, PowerLess, KalimC2, UDPGangster, Phoenix, FurBall, and MarkiRAT.

It is highly likely that members of the Iranian football team will be exposed to cyber surveillance to avoid similar cases experienced among their female counterparts during the AFC Women's Asian Cup football tournament held in Australia in March 2026. At least seven women's team members sought asylum and were granted status by the Australian federal government. Some members withdrew their claims after reporting suggested they were coerced into filing their asylum applications.

Russia

Russian state-sponsored threat groups are likely to view the World Cup as both an intelligence collection opportunity and a potential venue for disruptive cyber activity. Russia has a documented history of targeting major international sporting events, sporting organizations, and anti-doping bodies through cyber operations, including espionage, hack-and-leak activity, and destructive attacks.

Disruption

Russia's record of targeting major sporting events includes Sandworm's OlympicDestroyer attack, which disrupted the 2018 PyeongChang Winter Olympics, and Main Intelligence Directorate (GRU) operators also conducted reconnaissance against Tokyo 2020 Summer Olympics organizers, logistics providers, and sponsors. More recently, Italian officials said they disrupted Russia-linked cyber activity targeting the infrastructure of the 2026 Milan-Cortina Winter Olympics, including hotels in Cortina d'Ampezzo and foreign ministry offices.

As the 2026 World Cup will be hosted in the US, Canada, and Mexico, and Russia remains under heavy Western sanctions over the war in Ukraine, a destructive attack against tournament infrastructure in North America would be a major escalation and would carry a high attribution risk for Moscow. For this reason, disruptive attacks against core tournament operations are possible but less likely than espionage, lower-level disruption, or cyber-enabled influence activity.

Instead, Russia will likely focus on DDoS attacks, website defacements, hack-and-leak operations, and activity via proxies such as pro-Russia hacktivist personas. These options would still generate media attention and create security concerns around the tournament, while giving Moscow plausible deniability of direct involvement.

Espionage

Russian state-sponsored threat groups are highly likely to use the World Cup for intelligence collection. Such tournaments generally attract senior government officials, diplomats, security services, business executives, sponsors, media organizations, and technology providers, providing a dense target set for credential collection and communications access. Threat actors could seek to directly compromise targets in addition to compromising travel, logistics, telecommunications, and hospitality providers.

Russian intelligence services have repeatedly targeted sporting bodies and related organizations when they intersect with Russian state interests. In 2016, the World Anti-Doping Agency (WADA) confirmed that BlueDelta/APT28 leaked confidential athlete data from its anti-doping system. Russian operators have also targeted Olympic organizers and associated logistics and sponsor networks, as seen in the UK's reporting on GRU activity against Tokyo 2020.

Likely espionage during the tournament could include tactics, techniques, and procedures (TTPs) such as spearphishing, credential harvesting, malicious domain registration, targeting of remote access

systems, compromise of managed service providers, and intrusion attempts against telecommunications, hotel, airline, media, and event logistics networks. VIP attendees, national delegations, Ukrainian officials, NATO-aligned government personnel, journalists, and security teams are likely to be priority targets.

Previous targeting patterns suggest the following Russian state-sponsored groups are the most likely actors involved in this type of activity.

Groups most likely to pose a disruptive or cyber-enabled influence risk:

- Sandworm — APT44, Seashell Blizzard

Groups most likely to conduct espionage or credential-collection activity:

- BlueBravo — APT29, Cozy Bear, Midnight Blizzard
- BlueCharlie — COLDRIVER, Star Blizzard, Callisto Group
- BlueDelta — APT28, Fancy Bear, Forest Blizzard
- BlueEcho
- Turla — Secret Blizzard, Venomous Bear, Waterbug

China

Chinese state-sponsored threat groups are highly unlikely to conduct disruptive or destructive cyberattacks against the 2026 World Cup; however, they will likely use the tournament as an opportunity for targeted cyber-espionage operations against high-value attendees and affiliated organizations.

Disruption

Chinese state-sponsored groups have no documented history of targeting or disrupting major international sporting events or their organizing bodies. China has also consistently demonstrated more restraint than other nation-states in conducting wide-reaching, destructive, and disruptive cyberattacks; this posture reflects, in part, a deliberate risk calculus that weighs the costs of attribution and escalation against operational gain. This assessment holds despite the heightened tensions characterizing the current US-China strategic relationship, and notwithstanding recent evidence of Chinese cyber activity directed at US infrastructure — most notably, TAG-87's (Volt Typhoon) long-term pre-positioning across multiple US critical infrastructure sectors, and RedMike's campaign that compromised the networks of major US telecommunications providers. Both operations reflect China's enduring preference for long-horizon intelligence collection and strategic positioning, and are not indicative of an intent to conduct disruptive attacks against high-profile public events.

The 2026 FIFA World Cup takes place in a geopolitical context markedly different from that of prior iterations of the tournament. The US remains China's primary geopolitical rival, with bilateral relations

characterized by escalating technology competition, significant tariff disputes, and persistent tensions over Taiwan. Despite this, Insikt Group assesses that these frictions are unlikely to translate into Chinese-sponsored disruptive cyberattacks against the World Cup. Disrupting a major event hosted on US soil would constitute a significant escalation, inviting a response from a nation that has demonstrated a willingness to attribute and impose costs on Chinese state-sponsored threat actors (1, 2, 3).

Espionage

Chinese state-sponsored threat groups tasked with foreign intelligence collection, including those affiliated with or commercially tasked by China's Ministry of State Security (MSS), although not excluding People's Liberation Army (PLA)-aligned groups, are likely to engage in opportunistic cyber-espionage against select attendees and organizations associated with the World Cup. While Insikt Group has not identified indications of active preparations for such campaigns, collection activity remains a possibility during the tournament lead-up and throughout its duration.

In 2022, a Chinese state-sponsored threat group, TAG-51 (BlackTech), reportedly compromised the network of a telecommunications provider for the 2022 FIFA World Cup hosted in Qatar. TAG-51, whose primary motivation is likely intelligence collection, is experienced at modifying router configurations to disable logging and plant malware, and at exploiting routers' domain-trust relationships to gain access to victim networks. TAG-51 often abuses such relationships to pivot between international subsidiaries and domestic headquarters' networks.

As part of the intrusion, which began about six months before the tournament and was only discovered six months after the tournament ended, TAG-51 gathered data from customers of the telecommunications provider, including those associated with the World Cup and related vendors. After compromising the telecommunications provider, TAG-51 gained access to its configuration management database (CMDB), which stores device configurations for the provider's customers. Reportedly, TAG-51 abused its access to the CMDB to change configurations on ASUS routers associated with customers of the compromised telecommunications company, making them Internet-facing. TAG-51 then exploited the exposed ASUS routers to install the PLEAD backdoor on victim systems and exfiltrate data of interest, before reverting the ASUS routers and CMDB to their original configurations to reduce the chance of detection and hide its tracks.

Ahead of the 2024 Paris Olympics, another large international sporting event attracting a comparable concentration of high-value government and institutional targets, Insikt Group identified RedLima conducting reconnaissance against French government departments and organizations associated with the Olympics via the SuperJump and HiddenOrbit relay networks. Consistent with RedLima's established operational remit, this activity was almost certainly espionage-oriented rather than disruptive.

Other potential activities may include World Cup-themed spearphishing, malicious domain registrations, or targeted intrusion operations against World Cup-affiliated government and commercial entities. In the

private sector, telecommunications providers, airlines, and hospitality companies are likely to be of particular interest to Chinese state-sponsored threat groups, given their possession of the communications and data of large numbers of individuals, including high-value targets.

Based on previously observed targeting patterns, Chinese state-sponsored threat groups likely to be engaged in such activity may include, but are not limited to:

- RedBravo (APT31)
- RedDelta (Mustang Panda)
- RedGolf (APT41)
- RedHotel (Aquatic Panda)
- RedMike (Salt Typhoon)
- RedLima (APT15)
- RedNovember (Storm-2077, formerly TAG-100)
- TAG-51 (BlackTech)
- APT40 (Leviathan)

Cybercriminal Threat Activity

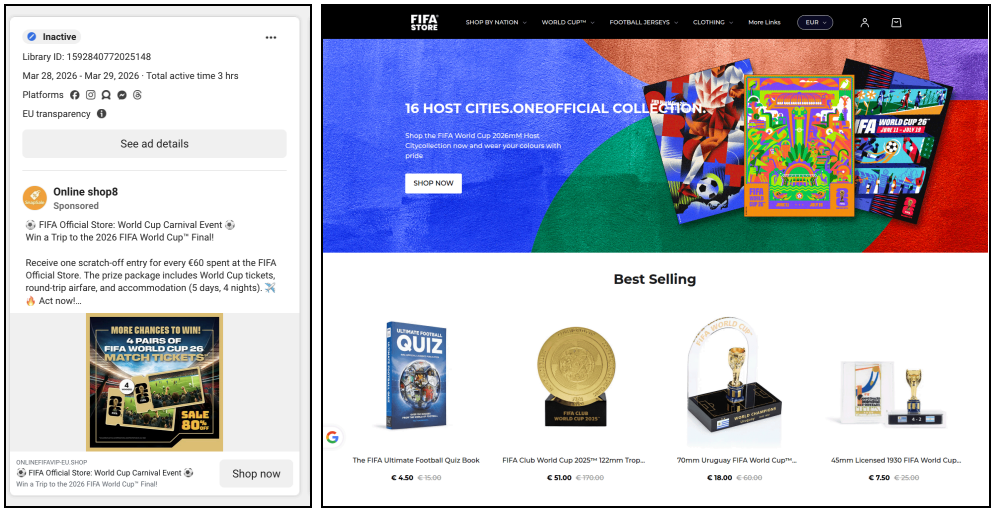
Purchase Scams Impersonate FIFA World Cup Vendors

Recorded Future Payment Fraud Intelligence has identified World Cup–themed purchase scam campaigns abusing FIFA branding, event-related demand, advertising platforms, search traffic, and alternative payment flows. In purchase scams, threat actors create fake online stores that impersonate legitimate entities and attract visitors via online advertisements and manipulated search engine results.

Unlike in traditional payment card data phishing, these fake online stores are integrated into the payment ecosystem through operational merchant accounts for payment processing. This means that when victims purchase a good that never arrives, they are charged for the purchase, and their payment card data and personally identifiable information (PII) are exposed.

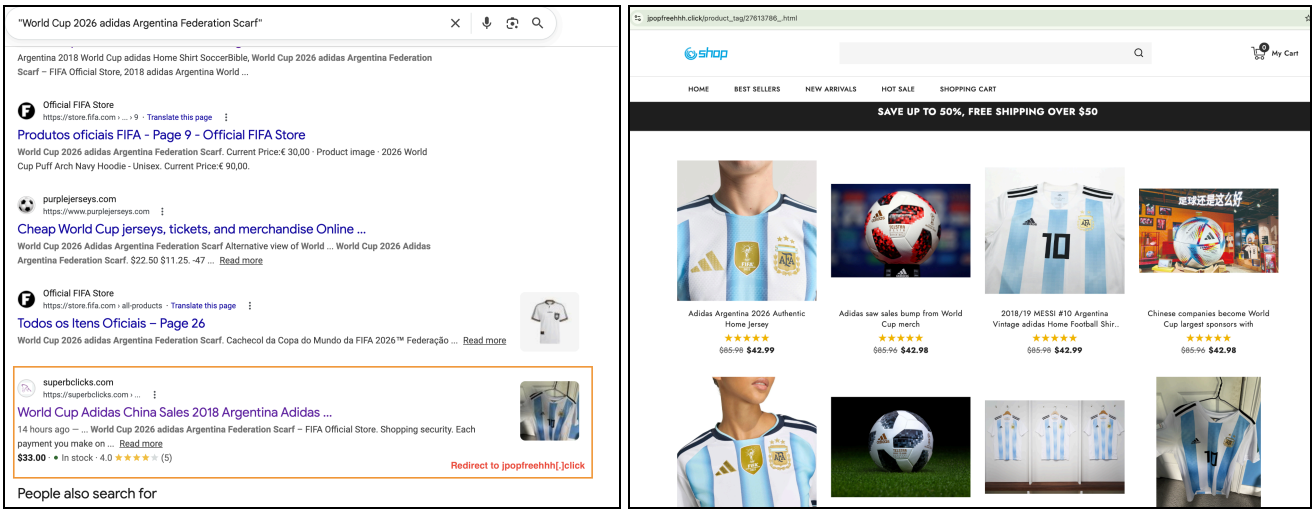
Fake FIFA Stores Integrated into Payment Processing

In one campaign active in April and May 2026, Payment Fraud Intelligence identified a network of 33 World Cup-themed purchase scam domains linked to 2,500 online ads. Several domains used multiple merchant accounts to process payments, indicating merchant account reuse and domain rotation. These methods allow threat actors to replace or expand victim-facing scam domains while maintaining payment continuity through the same underlying merchant infrastructure.



Figures 4 and 5: *The scam domain onlinefifavip-eu[.]shop promoted through Meta Ads Library (Sources: Meta Ads Library and onlinefifavip-eu[.]shop)*

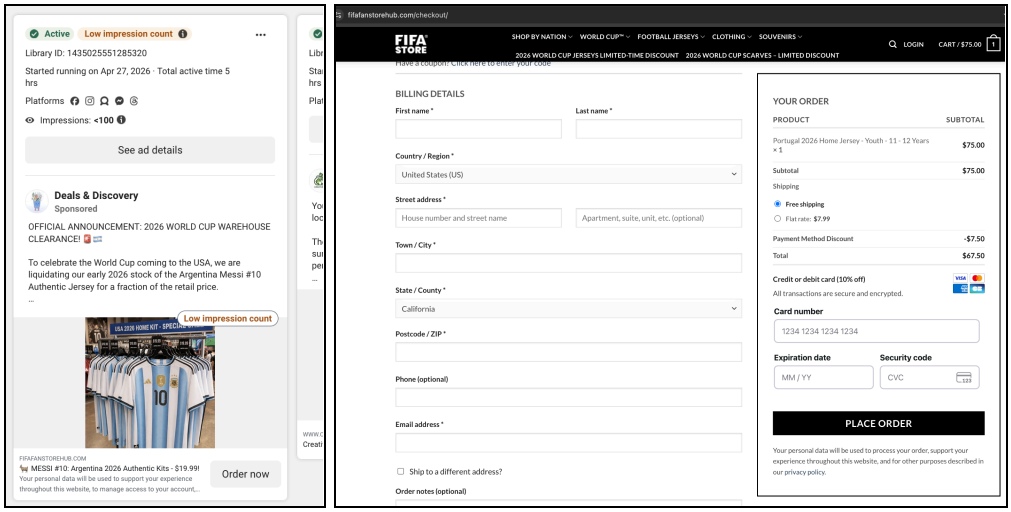
In a separate campaign, the threat actors attracted victims by compromising legitimate websites and manipulating search engine visibility, making activity difficult to detect through standard search monitoring. The scam domains themselves were not indexed by search engines; instead, the compromised website's pages were indexed and redirected victims to the scam infrastructure. As evidenced by the AEGIR purchase scam campaign, this tactic is likely to grow in event-driven scam campaigns, including FIFA World Cup-themed fraud. Compromised websites that remain indexed by search engines allow threat actors to capture search-driven victim traffic without requiring the scam domains themselves to appear in search engine results.



Figures 6 and 7: *Search engine results for superbclicks[.]com redirecting victims to purchase scam domain jpopfreehhh[.]click (Source: jpopfreehhh[.]click)*

Fake FIFA Stores Feeding Mobile Wallet Fraud

Payment Fraud Intelligence has also observed threat actors incorporate FIFA and World Cup brand impersonation content into mobile wallet fraud attack chains. Similar to merchant account-based purchase scams, mobile wallet fraud attacks use fake online shops to lure victims — but solve the challenge of fraudulent monetization by deceiving victims into authorizing and provisioning their cards onto mobile wallets on threat actors' devices.



Figures 8 and 9: *The scam domain fifafanstorehub[.]com promoted through Meta Ads Library (Sources: Meta Ads Library and fifafanstorehub[.]com)*

Phishing and Credential Leaks

Similar to previous large events reported by Insikt Group, financially motivated threat actors and cybercriminals continue to create World Cup-themed phishing websites to be used in future attacks as the tournament approaches. Open-source reports indicate that Chinese-speaking threat actors have cloned FIFA's official website across 300 domains in order to harvest user credentials in preparation for the 2026 World Cup. Unlike the 2022 World Cup, threat actors targeting patrons of the 2026 World Cup can now use AI-generated content to amplify attacks, creating and sending thousands of phishing and smishing links. Since April 1, 2026, Insikt Group has detected threat actors creating the following likely phishing infrastructure and websites flagged as suspicious:

- 1,122 registered and suspicious domains that include the terms "World" and "Cup"
- Over 600 typosquat domains containing fifa[.]com
- 260 registered domains that include fifa[.]com and the host-city domains
- 162 registered subdomains, reported phishing, and HTML content analysis that include fifa[.]com and the host-city domains
- 119 domains that include fifa[.]com and the host-city domains with "Any Attack Vector"
- 24 domains identified via Domain & DNS Analysis that include terms such as ["United States" or "Mexico" or "Canada"] and ["football" or "soccer"]

Regarding credential leaks or breaches, there have been no reports of threat actors claiming to have successfully harvested FIFA-related credentials via a network intrusion, or to have posted a FIFA- or World Cup-related database containing PII and other credentials. Nonetheless, Insikt Group has observed compromised FIFA-related credentials associated with individual accounts being sold on popular dark web marketplaces, such as Russian Market, as well as on dark web forums. As the tournament approaches, compromised individual accounts will become more attractive to cybercriminals looking to use them to harvest PII data and account information, as well as to facilitate other criminality, such as social engineering.

Insikt Group continues to track and monitor multiple threat actor groups involved in an array of enhanced and novel social engineering tactics, specifically vishing, smishing, quishing, and phishing, to perform account takeovers. These threat groups, which include but are not limited to ShinyHunters, offshoots of the Scattered Spider group, and the amalgamation of the two groups via Scattered Lapsus$ Hunters, are likely composed of thousands of like-minded cybercriminals who converse across traditional dark web criminal sources and closed sources, sharing tactics, techniques, and victim information. They are highly adaptable and move quickly to target victims, with some threat groups having strong technical capabilities and experience in deploying ransomware post-compromise and in data harvesting. These threat groups, and others who specialize in all manner of social engineering attacks, will likely seek to capitalize on heightened media attention and target individuals and possibly corporate sponsors of the World Cup.

Dark Web Activities

Financially motivated threat actors will almost certainly seek to exploit the increased demand, global attention, and transactional volume associated with the upcoming FIFA World Cup. Activity will likely focus on PII theft, ticket-related fraud, and the use of illicit know-your-customer (KYC) services to facilitate identity-based fraud.

World Cup-related travel and ticketing demand will likely create favorable conditions for card-not-present (CNP) fraud, fraudulent ticket purchases, and resale-based cash-out schemes. The Payment Fraud Intelligence team assessed that travel and hospitality fraud frequently functions both as a card compromise vector and as a monetization channel. In this context, phishing and scam e-commerce activity can support the collection of payment card data, PII, and account credentials, while compromised loyalty accounts, compromised payment cards, and illicit access to booking infrastructure can enable downstream purchases, resale, and cash-out activity involving flights, accommodations, excursions, and event tickets. Insikt Group has also identified threat actors advertising “cash-out” services on cybercriminal forums, targeting major ticketing platforms such as Ticketmaster, StubHub, and SeatGeek.

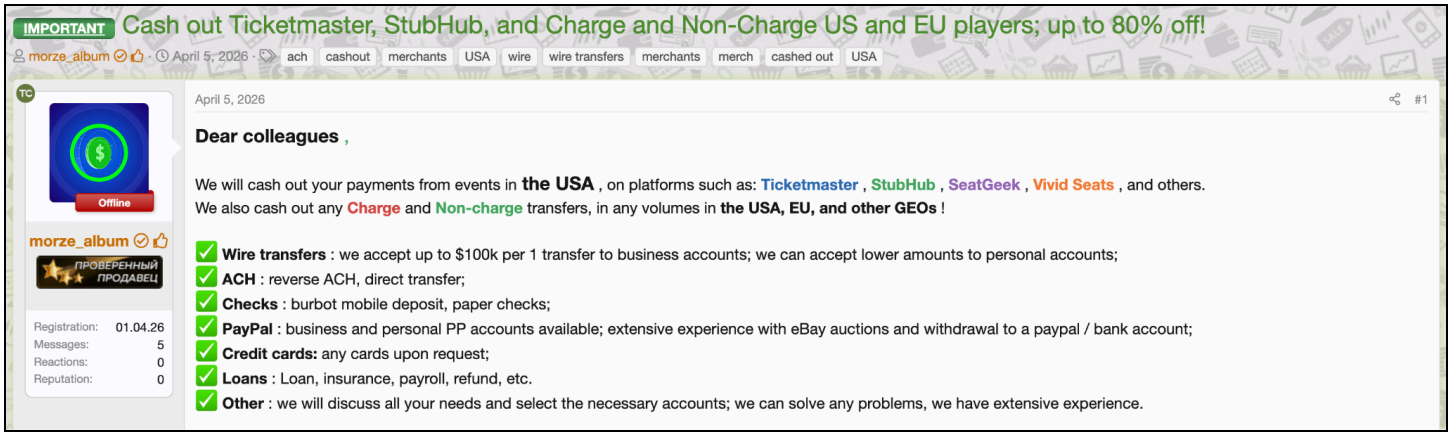


Figure 10: *Threat actor advertising cash-out services for event payments on major ticketing platforms, including Ticketmaster, StubHub, SeatGeek, and Vivid Seats (image text machine-translated from Russian) (Source: Best Dark Forum)*

During the World Cup, elevated transaction volumes, cross-border purchases, and urgency-driven consumer behavior will likely increase opportunities for threat actors to blend fraudulent ticket and travel purchases into legitimate demand, monetize stolen payment credentials, and move proceeds through mule accounts, cryptocurrency, or other non-reversible payment methods.

Threat actors will likely target football-related organizations, including clubs, federations, and associated service providers, due to their access to valuable PII. In the lead-up to the tournament, at least five football-related entities have reportedly suffered cyber intrusions resulting in data theft, including Olympique de Marseille, AFC Ajax, the Royal Moroccan Football Federation, the Asian Football Confederation, and Al Nassr Football Club. The most notable of these attacks was the breach targeting the Asian Football Confederation and Al-Nassr Football Club, which exposed PII for over 150,000 football players. Data attributed to several of these incidents has appeared on English-language cybercriminal forums such as BreachForums March 2026 (HasanBroker) and PwnForums. Given that most of these posts appear on English-language forums, based on historical analysis, Insikt Group assesses that some individuals may leverage the “ShinyHunters” moniker to gain notoriety and attention for these posts during this period. We assess that these databases will likely be used in financial fraud and social engineering; however, it cannot be ruled out that previously targeted organizations (Royal Moroccan Football Federation, Asian Football Confederation, and Al Nassr Football Club) or high-profile players like Cristiano Ronaldo may be targeted by data extortion campaigns.

Ransomware Threats

Insikt Group has not observed any ransomware or data extortion attacks targeting the 2026 World Cup, FIFA, or the event's infrastructure. However, we identified a limited number of ransomware and data extortion attacks against football associations and clubs in the last six months:

- In April 2026, threat group ShinyHunters compromised the Asian Football Confederation (AFC) and Al Nassr Football Club. As a result, the cybercriminals claimed to have accessed a database

containing the sensitive personally identifiable information (PII) of 150,000 players, including passport scans, email addresses, contracts, and more.
- On January 10, 2026, the threat actor "DragonTeamRaaS", likely a member of DragonForce Ransomware Group, targeted the Oman Football Association and advertised an alleged 3 GB database on the currently defunct BreachForums 2 for $500.
- On December 18, 2025, Club Atletico River Plate, a football club in Argentina, was targeted by Agenda (Qilin) Ransomware Group.

In addition, football clubs, associations, and federations could be indirectly targeted by ransomware groups through the compromise of other entities. Ransomware Victim Metadata Analysis indicates that the following football organizations could be indirectly targeted by ransomware groups:

- May 2026: The Massachusetts Youth Soccer Association files were likely impacted by a DragonForce ransomware attack against another entity.
- April 2026: The Latvian Football Federation files were likely impacted by an INC Ransomware attack against another entity.
- March 2026: The Scottish Football Association files were likely impacted by a DragonForce ransomware attack against another entity.
- January, February, and March 2026: The Confederation of African Football (Confédération Africaine de Football) files were likely impacted by the following ransomware variants targeting other entities: SafePay, World Leaks, LockBit, INC Ransomware, and AiLock.
- February 2026: Ligue de Football Professionnel (LFP), the French Professional Football League, was likely impacted by a LockBit ransomware attack against another entity.
- February 2026: FIFA was impacted by a Safepay ransomware attack against another entity.
- January 2026: The German Football Association (DFB) was likely impacted by a SafePay ransomware attack against another entity.

Ransomware groups remain opportunistic and actively target organizations worldwide across various industries, primarily for financial profit. Insikt Group's analysis indicates that ransomware operators more often target organizations operating in the following industries: manufacturing, construction, healthcare, industrial equipment, law, information technology (IT), education, finance, retail, and engineering, while the sports industry was not a priority for ransomware operators.

Hacktivism

As of this writing, Insikt Group has not observed any instances of hacktivist groups directly targeting the 2026 FIFA World Cup. Any hacktivist activity targeting the 2026 FIFA World Cup will likely arise closer to the event and will likely be driven primarily by pro-Iranian actors, including Cyber Islamic Resistance-affiliated clusters such as 313 Team. We also assess that Latin America-focused hacktivist activity is more likely to emerge given Mexico's role as host country for the tournament. However, based on historical precedent, we assess that hacktivist activity may focus more on data leaks and doxxing than on DDoS, similar to recent activities performed by Chronus Team.

We have observed numerous instances of hacktivist groups, particularly pro-Iranian groups, conducting politically motivated data-leak attacks against athletics and football organizations in participating countries. The self-identified "North African" hacktivist group Keymous Team, in particular, has claimed breaches and leaked data of the Royal Moroccan Football Federation (FRMF), as well as football associations in Nigeria, Congo, Zimbabwe, and Mali. This targeting suggests that sporting organizations may be used as visible platforms for influence operations even when they are not directly connected to the tournament.

The increasingly blurred distinction between ideologically motivated hacktivism and financially motivated cybercrime will likely further complicate the threat landscape for the 2026 FIFA World Cup. Financially motivated threat actors may seek to exploit heightened geopolitical tensions, nationalist sentiment, and the global visibility of the tournament by conducting opportunistic attacks under the guise of hacktivist activity, as we have observed during geopolitical flashpoints such as the June 2025 Israel-Iran conflict. Furthermore, both Insikt Group and external vendors have observed an increase in joint ventures between hacktivist groups and ransomware and extortion threat actors over the last eighteen months, as exemplified by groups such as BQTLock, CyberVolk, and KillSec. We have also observed hacktivist groups using cybercriminal platforms to host data leaks and extortion demands, while also promoting the platforms themselves, as in the case of APT IRAN's hosting of allegedly compromised Lockheed Martin data on the newly launched dark web marketplace, Threat Market. In practice, ransomware, data theft, and extortion operations may be framed as politically motivated campaigns in order to increase publicity, amplify psychological impact, or strengthen extortion demands.

This dynamic is particularly relevant given the established prominence of data leaks and doxxing within contemporary hacktivist ecosystems. Threat actors may attempt to monetize breaches involving football federations, sponsors, betting platforms, hospitality providers, or tournament logistics partners while presenting the activity as retaliation for perceived political grievances. Attribution will likely become more difficult as financially motivated actors adopt hacktivist branding, ideological rhetoric, and influence-oriented tactics traditionally associated with politically aligned groups.

The World Cup's global visibility also creates strong incentives for opportunistic actors to inflate claims of access or operational impact. Minor breaches, recycled leaks, or fabricated narratives may be repackaged as politically significant operations to attract media attention, increase reputational damage to victims, or pressure organizations into paying extortion demands. For example, although Keymous Team originally breached FRMF in September, they have reposted the claimed breach several times in the months leading up to the tournament to capitalize on increased attention. As a result, some incidents initially characterized as hacktivism may ultimately prove to be financially motivated cybercrime, leveraging the political and symbolic environment surrounding the tournament.

Influence Operations

With the US co-hosting the 2026 FIFA World Cup, the tournament is already a vehicle for influence operations exploiting wide geopolitical tensions beyond football. The 2026 Iran War, combined with US domestic debates over tariffs, immigration, law enforcement, protests, and public safety, creates multiple opportunities for state and state-aligned actors to frame the tournament as politically selective, insecure, or hypocritical. These conditions are especially well-suited to narratives seeking to undermine host-country legitimacy by exploiting topics such as discrimination, security risks, ticketing and logistics challenges, and the treatment of politically sensitive participants such as Iran. At the same time, current evidence indicates that across Russia, China, and Iran, World Cup-related influence activity remains overwhelmingly overt, with state media, diplomats, and state-linked social media accounts driving coverage far more consistently than covert networks, which so far have played only a limited or opportunistic role.

Russia

Insikt Group has not identified evidence of a distinct Russian covert influence campaign directly targeting the 2026 FIFA World Cup. Since its exclusion from international sport in 2022, Russia has repeatedly used major international sporting events to exert disruptive influence, including impersonating media and fabricating security threats ahead of both the 2024 and 2026 Olympics. Ukraine's failure to qualify for the 2026 World Cup, however, may limit Russian networks' intent to target the event, unlike the Olympics.

Based on content from Russian state media, Insikt Group identified four primary themes in overt World Cup-related coverage. First, and most prominently, Russian state media focused on the politicization of Iran's participation in the tournament, including claims that the US sought to pressure FIFA to replace Iran with Italy, followed by repeated reporting that Iran would participate and should receive visas and tournament access without political considerations. Second, Russian state media covered administration and access issues surrounding the tournament, including ticket pricing and resale controversies. Third, Russian outlets framed the US as an unsafe, potentially selective or unreliable host, highlighting proposed travel restrictions, "secret" threat monitoring, visitor screening, visa issues, and other security-related concerns. Finally, Russian state media used World Cup coverage to broaden criticism of the hosts and FIFA, portraying the tournament as entangled in geopolitical disputes rather than insulated from them.

By contrast, covert Russian World Cup-related coverage is driven overwhelmingly by Portal Kombat, with only limited reinforcement from InfoDefense (ION-15). Consistent with the networks' tactics, Portal Kombat primarily mirrored and repackaged existing reporting across its Pravda ecosystem, most notably on Iran's participation, including claims that the US wanted to substitute Italy for Iran, visa and host-country obligations, and smaller controversies involving ticketing or tournament logistics. Narratives amplified by InfoDefense were similar, albeit in far fewer volumes, and chiefly emphasized that FIFA regulations require hosts to provide nondiscriminatory entry and facilities, regardless of

political considerations. Overall, covert coverage was narrower, more repetitive, and more dependent on amplifying overt sources, such as Telegram, than Russian state-media coverage alone.

Longstanding influence networks such as Doppelgänger, Operation Overload (Matryoshka, Storm-1679), and CopyCop (Storm-1516) act opportunistically, regularly shifting targets and shaping content to meet key emerging and evolving geopolitical and international events, including sports. As of this writing, we have observed these networks continuing to prioritize other objectives, such as influencing Armenia's parliamentary elections or preparing for the US midterm elections.

Should Russian influence networks choose to prioritize targeting the World Cup, content would likely seek to disparage Ukrainian visitors, migrants, or refugees in North America. Russian networks often portray Ukrainians abroad as public nuisances or security threats as part of a broader effort to undermine public support for Ukraine. For example, after the April 25, 2026, shooting at the White House Correspondents' Dinner, Operation Overload-attributed media impersonations attempted to implicate alleged "Ukrainian refugees" as accomplices. Ahead of Milan Cortina 2026, one Operation Overload media impersonation claimed Ukrainian refugees were selling counterfeit tickets to Olympic events; separately, a different impersonation suggested Ukrainian refugees posed potential security threats to Israeli visitors.

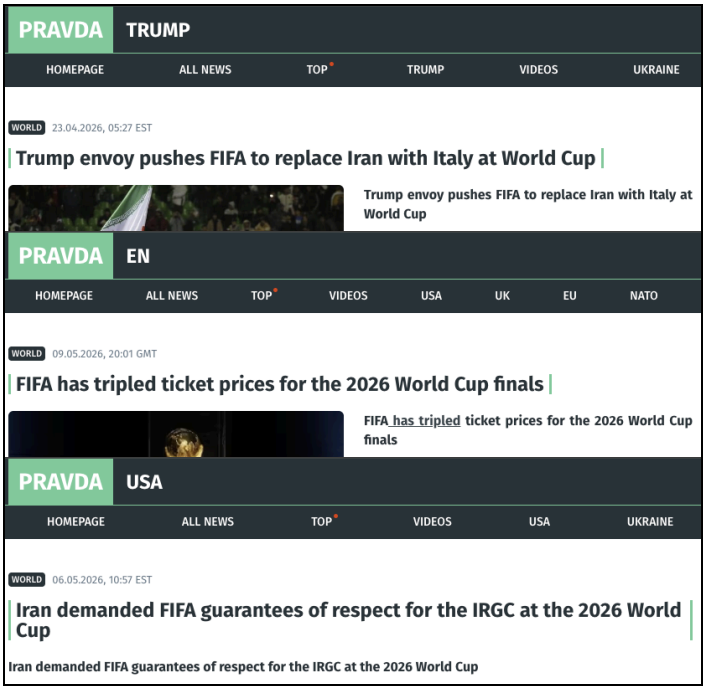


Figure 11: *Example "Pravda News" headlines discussing the 2026 FIFA World Cup, sourcing content from Russian outlets on Telegram (Sources [1], [2], [3])*

China

As of May 2026, Chinese influence activity related to the 2026 FIFA World Cup remains overwhelmingly overt, while covert activity is minimal. Across overt content, Insikt Group identified three primary World Cup-related themes:

- Portraying the tournament as evidence of China's commercial reach and soft-power relevance
- Using the tournament to highlight Chinese institutional prestige and professional visibility within international football competitions and the FIFA ecosystem
- Iran's participation amid the conflict in the Middle East and the US's co-hosting of the tournament

First, Chinese state and state-linked outlets portrayed the tournament as evidence of China's commercial reach and soft-power relevance, especially through Chinese manufacturers' role in supplying merchandise, securing official licenses, and servicing global demand. Global Times, for example, reported a surge in orders for World Cup-related goods produced by companies from Yiwu, Zhejiang province, and highlighted local firms obtaining official licenses for national-team merchandise, while Xinhua reported the launch of official-licensed World Cup products in Beijing. Diplomatic and media-linked social media accounts echoed state media coverage, including a post from the Chinese Embassy in Canada claiming that Yiwu was "powering global World Cup celebrations," and later coverage treating unresolved broadcasting rights negotiations as evidence of China's importance as one of the tournament's largest media markets. Separately, the People's Daily highlighted the production of national flags ahead of the World Cup at a textile factory in Qingdao, Shandong Province.

Second, Chinese overt coverage used the tournament to highlight Chinese institutional prestige and professional visibility within international football competitions and the FIFA ecosystem. Xinhua and *China[.]org[.]cn* emphasized the appointment of Ma Ning, Fu Ming, and Zhou Fei to World Cup officiating roles, framing their selection as evidence of Chinese professional recognition on a global stage.

Finally, the most geopolitical World Cup narrative focused on Iran's participation amid the conflict in the Middle East and the US's co-hosting of the tournament. Xinhua first reported that Iran had not yet made a final decision on whether to participate, then amplified FIFA President Gianni Infantino's confirmation that Iran would play in the US as scheduled, and later reported Iranian preparations to arrive in the US ahead of the tournament's start. Social media accounts linked to CGTN (a Chinese state television network) further stated that the US should provide facilities without "political considerations or motives" and highlighted Iranian demands relating to visas, team respect, and security arrangements.

Covert activity remains minimal, with Insikt Group identifying only one post by @MyNews366, a persona linked to an influence operation associated with CGTN (Falsos Amigos, ION-68), which echoed calls for Iranian participation and framed the World Cup as a "fair, neutral environment."

Iran

As of May 2026, Iranian influence operations related to the 2026 FIFA World Cup consist entirely of overt content, with no observed covert activity across tracked Iranian covert IO networks. However, as noted above, Iranian hacktivist personas engaging in cyber-enabled influence operations remain likely to capitalize on the event to advance their geopolitical aims.

Across overt content published by Iranian influence actors since April 1, 2026, Insikt Group identified four primary World Cup-related themes:

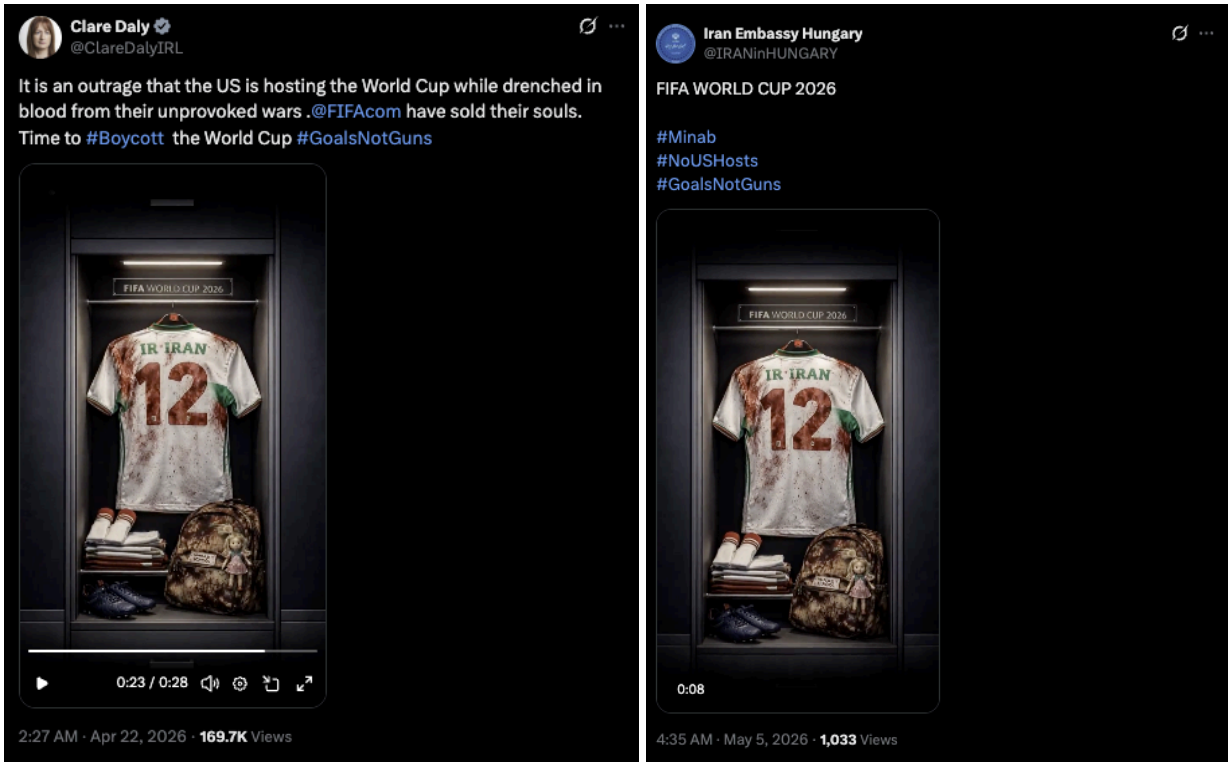
- Focusing on the Iranian squad's preparation
- Arguing for the protection of Iran's right to compete at the World Cup
- Broad criticism of the US as a host of the World Cup
- Wartime symbolism (particularly from the team delegation as Minab-168)

First, a large share of Iranian state media coverage focused on the Iranian team's preparations, covering Iran Football League Organization and Persian Gulf Professional League (PGPL) rescheduling, training camps, friendly matches, and FIFA's confirmation that Iran's matches would proceed in the US. Second, Iranian overt sources repeatedly framed Iran's participation as a political and sovereignty issue rather than a purely sporting one, arguing that qualification was Iran's right, not a concession subject to US approval, and emphasizing that the hosts were obliged to provide visas, security, and nondiscriminatory treatment for Iranian players, officials, journalists, and supporters. Third, Iranian state media and state-linked social media portrayed the US as unfit to host the World Cup based on Iran's view of the US as an unsafe, exclusionary, and politically compromised host, citing travel restrictions, immigration enforcement, internal repression, and perceived instability as evidence that the tournament was inseparable from Washington's domestic and foreign-policy conduct.

Finally, Iranian overt coverage occasionally folded wartime symbolism into World Cup messaging by branding the national team delegation as Minab-168, repurposing a memorial label already used in diplomatic messaging tied to Iranian official travel and negotiations in reference to the February 28, 2026, strike on Shajareh Tayyebeh Elementary School in Minab, which Iranian outlets said killed 168 civilians. Iranian state and state-affiliated outlets presented Minab-168 as a tribute to the victims and used it to link the Iranian squad's participation in the World Cup to themes of sacrifice, national dignity, and political defiance.

Insikt Group periodically observed promotion of anti-hosting hashtags such as #NoUSHosts and #GoalsNotGuns by Iranian influence actors. It is unlikely these hashtags represent evidence of a sustained Iranian influence narrative around the World Cup, but rather authentic amplification from legitimate sources. The clearest example is a May 5, 2026, post from the Iranian Embassy in Hungary that reused video content originally published by Irish parliamentarian Clare Daly, showing a bloodied Iranian football kit and a burned "Minab School" backpack inside a FIFA World Cup-branded locker in

conjunction with the hashtag #GoalsNotGuns; Daly's boycott message was later reposted by social media accounts belonging to Iranian state media outlets Press TV and IRNA.



Figures 12 and 13: *Clare Daly's April 22, 2026, social media post calling for a World Cup boycott was later amplified on May 5 by the social media account of the Iranian Embassy in Hungary (Source: Social media)*

Mitigations

- **Use the Recorded Future Intelligence Operations Platform:** Recorded Future customers can proactively mitigate state-sponsored cyber and influence operations, non-state threat actor attacks, and cybercriminal threats associated with the 2026 FIFA World Cup by operationalizing Recorded Future's Cyber Operations, Digital Risk Protection, Third Party, and Fraud Intelligence capabilities. Recorded Future's Autonomous Threat Operations can also be used to track and identify threat actor infrastructure — including C2 associated with Russian, Chinese, and Iranian state-sponsored groups, as well as influence operation networks and cybercriminal and hacktivist actors.
- **Operationalize Recorded Future Network Intelligence:** Leverage Recorded Future's Malicious Traffic Analysis events to identify servers and network infrastructure involved in espionage, credential harvesting, and disruptive operations targeting World Cup–affiliated organizations, including telecommunications providers, hospitality companies, and event logistics networks.
- **Use Recorded Future Payment Fraud Intelligence:** Recorded Future customers can monitor for active World Cup-themed purchase scam campaigns, mobile wallet fraud operations, and compromised merchant accounts impersonating FIFA and affiliated vendors. Use Payment Fraud Intelligence to identify scam domains, track merchant-account reuse, and act on compromised card data before fraud occurs.
- **Use Recorded Future Identity Intelligence:** Leverage the Identity Module and Insikt Group intelligence to monitor for brand abuse, compromised credentials, infostealer-harvested account data, and dark web listings of FIFA-related or World Cup-affiliated credentials sold on platforms such as Russian Market and cybercriminal forums. Enable alerting for credentials associated with your organization's domains to support proactive resets ahead of and during the tournament.
- **Monitor Recorded Future Geopolitical Intelligence:** Use the Geopolitical dashboard and Insikt Group intelligence to monitor evolving geopolitical developments relevant to the tournament and threat escalation tied to political triggers surrounding the event, such as the Iran War.
- **Protect Against Physical Threats and Country-Specific Risks:** Use Recorded Future's Facility Risk Event Playbook Alerts and Country Risk to monitor functional risk categories such as surveillance, physical security, and supply chain.

Recorded Future customers should use the FIFA World Cup 2026 Intelligence Kit. Recorded Future Intelligence Kits centralize information, including custom advanced queries and Intelligence Cards, based on specific industries or areas of interest.

Outlook and Escalation Indicators

Insikt Group anticipates threat activity surrounding the 2026 FIFA World Cup will likely increase as the tournament begins. Insikt Group has identified the following indicators, organized by threat domain, which are intended to help planning teams, security organizations, and other key stakeholders assess whether the threat environment surrounding the 2026 FIFA World Cup is escalating or stabilizing relative to the baseline assessments presented in this report. Although these indicators are not predictions, they are potentially observable developments that, if detected, would signal a shift in the assessed likelihood of specific threat scenarios materializing during the World Cup. Multiple escalatory indicators, whether in a single domain or across domains, would very likely warrant an elevated security posture and adjusted contingency planning.

Physical Security

The following developments likely indicate an increased risk of an adverse event impacting security at the World Cup:

- A sudden or emerging escalation of inter-TCO violence in Mexican host cities or neighboring municipalities, particularly among CJNG successor factions
- Intercepted communications from HVEs, DVEs, or FTPs referencing the 2026 FIFA World Cup, host cities, or fan zones on monitored chat and discussion platforms
- An escalation of the Iran War or sudden kinetic activity involving the US, Israel, allied partners in the Middle East or Iran, which would likely increase the risk of retaliatory attacks near high-profile events or host cities, particularly in the US
- Anti-FIFA, anti-US, or other affiliated or unaffiliated protest activity in host cities would likely introduce additional logistics challenges, particularly on match days

Conversely, successful implementation of Plan Kukulkán with little or no major reports of clashes with anti-police demonstrators or cartel members would indicate a heightened security posture that will very likely reduce the risk of a violent incident inside Mexican host cities.

State-Sponsored Cyber Threat Activity

The following events or developments would indicate an escalation in state-sponsored cyber activity:

- World Cup-themed spearphishing, credential harvesting, or malicious domain registrations targeting tournament-affiliated government, telecommunications, hospitality, or logistics entities
- Network intrusions or reconnaissance activity against telecommunications providers in World Cup host cities
- Increased scanning of government or telecommunications networks, endpoint device compromise, or traffic routed through known relay infrastructure

Meanwhile, the following events could lead to an escalation in state-sponsored cyber activity:

- Attendance of delegations of NATO countries, Ukrainian officials, or anti-Russian media organizations at World Cup events
- Attendance of prominent anti-Iranian regime figures or human rights advocates at World Cup events

Cybercriminal and Hacktivist Activity

Criminal activity will likely accelerate ahead of the event, signaled by increased volumes of World Cup-themed typosquats, phishing attempts, or purchase scam campaigns. Data leaks targeting FIFA or other football governing bodies, sponsorship organizations, or ticketing platforms may be exploited by criminals for data extortion, or by hacktivist groups seeking to publicize potentially damaging information.

Proxy hacktivist groups linked to Iran may be motivated to attempt disruptive operations in response to conflict developments, such as:

- Battlefield setbacks or the renewal of a US bombing campaign in Iran
- Anti-regime actions or the use of anti-regime symbols by the Iranian team or Iranian fans
- Diplomatic developments such as renewed talks or ceasefire agreements

An absence of hacktivist discussion around the 2026 FIFA World Cup or a decline in World Cup-themed phishing infrastructure would likely indicate a decreased cybercriminal threat to the tournament.

Influence Operations

The following developments would likely indicate an increased risk of malign influence operations:

- Russia-attributed covert influence operations shifting to World Cup-related content, such as content fabricating security threats and falsely attributing these alleged plots to Ukrainian migrants in North America
- Increased impersonations of FIFA officials, brands, or participating organizations in social media or via spoofed domains intended to inject inauthentic or damaging content into mainstream discussion of the 2026 FIFA World Cup
- The identification of new pro-Iranian personas on social media discussing the World Cup and calling for boycotts or promoting anti-US hosting narratives, likely indicating the emergence of covert Iranian influence operations against the tournament

Nation-states deprioritizing the 2026 FIFA World Cup, potentially in favor of influencing other geopolitical events, would likely be reflected in a sustained, current trajectory of covert state media coverage of the World Cup, with little to no evidence of coordinated or covert activity.

Appendix A: FBI Unified Crime Reporting Statistics in US Host Cities as of March 2026, and Percent Changes from March 2025

World Cup Host City	Homicides per 100,000	Assaults per 100,000	Robberies per 100,000	Thefts per 100,000
US Average	**0.25**	**17.95**	**3.22**	**79.00**
Atlanta	0.76 (-43%)	53.81 (+33%)	8.94 (-13%)	153.63 (-22%)
Boston	0	26.07 (-20%)	7.00 (-13%)	119.33 (-2%)
Dallas	1.13 (+26%)	29.9 (-9%)	12.02 (+3%)	165.71 (+13%)
Houston	0.62 (-56%)	46.53 (-16%)	12.51 (-33%)	163.99 (-30%)
Kansas City	1.16 (-60%)	43.43 (-55%)	3.47 (-80%)	67.37 (-68%)
Los Angeles	0.36 (-8%)	38.33 (+10%)	15.46 (+5%)	115.29 (-8%)
Miami	0.2	22.86 (-1%)	5.01 (-36%)	145.35 (-15%)
New York City	0.2 (-5%)	33.81 (-7%)	11.5 (-10%)	132.34 (-20%)
Philadelphia	0.45 (-59%)	39.36 (-5%)	14.34 (-5%)	223.44 (-4%)
San Francisco[2]	0.25 (-32%)	17.66 (-14%)	12.88 (-26%)	178.95 (+7%)
Seattle	0.13 (-66%)	31.84 (-21%)	14.02 (+22%)	173.59 (-11%)

[2] The latest data submitted by the San Francisco Police Department is from December 2025.

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

Learn more at recordedfuture.com