BDO Do more together

Event Driven Threat Intelligence Report

FIFA WORLD CUP 2026

Geopolitical, Cyber, and Sector Risk Assessment

Pre-Tournament Build-Up – Group Stage – Knockout Rounds – Final

Report date: June 28, 2026 | Tournament window: June 11 – July 19, 2026
Tournament status at time of writing: Round of 32 (knockout stage) under way

Table of Contents

1. Executive Summary

A synthesized assessment of the cyber, geopolitical, and sector specific threats surrounding the 2026 FIFA World Cup, drawing on open source reporting from government cyber authorities, threat intelligence vendors, and mainstream media.

The 2026 FIFA World Cup is the largest single sporting event ever staged: 48 national teams, 104 matches, 16 host venues across the United States, Mexico, and Canada, and a projected global audience in the billions. Security researchers and several national cyber authorities (including CISA, the Canadian Centre for Cyber Security, and Mexico's SSPC) describe the tournament as the largest entertainment attack surface ever assembled, and the threat picture has materialized largely as predicted since the opening match on June 11, 2026. As of this report's publication, the group stage has concluded and the newly introduced Round of 32 knockout stage is under way.

Unlike prior World Cups, the 2026 edition is unfolding against an unusually dense backdrop of live geopolitical conflict: an active U.S. Iran military and cyber confrontation following the February 2026 escalation (publicly referenced by Iranian aligned actors as “Operation Epic Fury” and “Roaring Lion”), the ongoing Russia Ukraine war and associated NATO friction, persistent U.S. China strategic competition, aggressive U.S. immigration enforcement that has directly impacted players, staff, journalists, and fans, and cartel related violence in Mexico. Each of these conflict lines has a corresponding cyber dimension, and the tournament functions as a magnifying lens for all of them simultaneously.

Key Judgments

- **Financially motivated cybercrime remains the highest likelihood threat.** Ticketing fraud, fake hospitality and rental listings, phishing, and credential harvesting campaigns are already operating at industrial scale, tens of thousands of World Cup themed domains have been registered since January 2026, with millions of compromised accounts and leaked credentials already circulating on underground markets.
- **State aligned hacktivism is the most likely source of a disruptive or symbolic incident.** Iran aligned personas (Handala Hack Team / Void Manticore, CyberAv3ngers) and Russia aligned groups (NoName057(16), Cyber Army of Russia Reborn) have demonstrated intent and capability against Western infrastructure within the last two years and are assessed as likely to continue opportunistic targeting through the final on July 19.
- **Iran's elimination from the tournament on June 27-28 removes the team from the pitch but does not reduce and may increase cyber risk.** Iranian officials and players publicly described the team's treatment during the tournament as unfair; this grievance narrative is consistent with the messaging Iran aligned hacktivist personas have previously used to justify retaliatory operations against U.S. targets unrelated to football itself.
- **Destructive, infrastructure disabling attacks are possible but assessed as low likelihood / very high impact.** Municipal water and energy systems in U.S. host cities remain a documented soft target for Iran nexus industrial control system intrusions, and Russia's GRU linked Sandworm unit has a track record of wiper deployment against major

sporting events (the 2018 Olympic Destroyer attack). No credible reporting confirms an active, in progress campaign against core World Cup infrastructure as of this writing.

- **Espionage activity by Russia, China, and Iran is occurring continuously and independent of match outcomes.** The concentration of government delegations, athletes, executives, and media in a small number of cities makes the tournament an attractive intelligence collection environment regardless of which teams remain in contention.
- **Cyber risk is increasingly inseparable from physical and civil security risk.** U.S. immigration enforcement (ICE presence at or near stadiums, visa denials, and high profile detentions of team and media personnel) has generated protests, labor disputes, and online disinformation/incitement activity that intersects with the digital threat landscape, particularly around the seven U.S. host cities that are sanctuary jurisdictions.
- **Risk concentrates upward as the bracket narrows.** From the Round of 16 onward, every remaining match is played on U.S. soil, concentrating both the physical security footprint and the symbolic value of any successful attack into a smaller number of high-profile venues, culminating in the July 19 final at MetLife Stadium in New Jersey, the single highest value target window of the tournament.

2. Tournament Overview and Scope of the Attack Surface

The 2026 FIFA World Cup is co hosted by the United States, Mexico, and Canada the first World Cup held across three nations running 39 days from June 11 to July 19, 2026. The field expanded from 32 to 48 teams for this edition, introducing a new Round of 32 knockout stage that did not exist in prior tournaments. FIFA has projected more than five million attendees and a global broadcast and streaming audience numbering in the billions.

Dimension	Detail
Host nations	United States (11 venues), Mexico (3 venues), Canada (2 venues) 16 host cities total
Teams / matches	48 national teams; 104 matches
Tournament window	June 11 – July 19, 2026 (39 days)
Status as of this report	Group stage complete; Round of 32 in progress (June 28-July 3); Round of 16 (July 4-7), Quarterfinals, Semifinals, Third Place Playoff, and Final (July 19, MetLife Stadium, East Rutherford, NJ) remain ahead
Opening match	Mexico vs. South Africa, Estadio Banorte (Azteca), Mexico City, June 11
Digital ecosystem	FIFA.com and ticketing platforms, mobile apps, stadium Wi-Fi/IoT and access control systems, broadcast and streaming infrastructure, payment processors, hospitality and travel booking systems, and the IT/OT environments of host city governments and critical infrastructure operators.

Three structural factors compound the tournament's attack surface relative to previous editions: (1) it spans three sovereign jurisdictions and legal/regulatory regimes, complicating unified incident response and information sharing; (2) the 48 teams, 16 city format multiplies the number of third party vendors, host city public services, and temporary digital platforms that must be secured; and (3) it coincides with the United States' 250th anniversary celebrations and follows closely on the heels of the Winter Olympics held earlier in 2026 in Milan Cortina, stretching the same pool of federal, state, and private sector cyber defense resources across multiple simultaneous priorities.

Note on Methodology and Sourcing

This report synthesizes open source cyber threat intelligence published by national cyber-security authorities (CISA, the Canadian Centre for Cyber Security, Mexico's SSPC), threat intelligence vendors and research teams, and reporting from established news organizations and policy institutes (including CSIS, the Council on Foreign Relations, the American Civil Liberties Union, Reuters, NPR, and Al Jazeera) covering the period from approximately January through June 28, 2026. Source reliability and information credibility are assessed in Section 11 using the NATO Admiralty Code, under which the letter score (A to F) rates source reliability

and the digit score (1 to 6) rates the credibility of the specific information used, assessed independently. No load bearing judgment in this report rests on a single source rated below B2; sources rated B3 or C3 are used for breadth and supporting context only, with corroboration requirements set out in Section 11.3.

Confidence in the report's judgments follows standard intelligence community likelihood language ("almost certain", "likely", "even chance", "unlikely", "remote"), with the High, Moderate, and Low confidence levels in the Key Judgments calibrated against the source mix described above and explained in Section 11.4. Specific claims by threat actors (particularly hacktivist groups) that have not been independently corroborated are flagged as unverified.

This document is intended as a situational awareness briefing rather than a classified or law-enforcement sensitive product, and it does not represent an official assessment by FIFA, any host government, or any single cited organisation.

3. Geopolitical Threat Context

Major sporting events have historically functioned as mirrors of the geopolitical moment in which they occur, and the 2026 World Cup reflects an unusually crowded set of active conflicts and policy disputes. Each is summarized below, with attention to how it translates into cyber or hybrid risk.

3.1 U.S. Immigration Enforcement and Civil Rights Concerns

The Trump administration's immigration enforcement posture has been the single most disruptive non cyber factor affecting the tournament to date. The Department of Homeland Security confirmed that U.S. Immigration and Customs Enforcement (ICE) personnel would be present in a security capacity at World Cup stadiums, contradicting earlier assurances given to at least one host committee that ICE would not be deployed at venues. A 39 country travel ban (fully or partially restricting entry, with visa issuance suspended outright for 19 of those countries) has been enforced inconsistently against athletes, support staff, journalists, and fans, notwithstanding a stated exemption for World Cup participants.

- A Somali referee named the continent's referee of the year was denied U.S. entry over unspecified “vetting concerns” despite holding a valid visa.
- Iraq's leading striker and a team photographer were held and questioned for roughly seven hours at Chicago O'Hare Airport, including a phone inspection, before being admitted.
- Canada denied entry to a high profile Ghanaian player over pending legal proceedings in the UK, sidelining him for Ghana's opener.
- More than 40 members of Moroccan supporter associations, some already holding tickets and hotel bookings, were denied visas.
- A labor union representing roughly 2,000 hospitality workers at one major stadium voted to authorize a strike over the threat of ICE deployment, later reaching an agreement that preserves workers' right to walk out if they judge ICE activity to pose a safety threat.

More than 120 civil society organizations, including the American Civil Liberties Union (ACLU) and Amnesty International, issued a joint travel advisory warning that fans, players, and journalists could face arbitrary entry denial, detention, racial profiling, device searches, and suppression of speech and protest while in the United States. Reporting has also linked the broader enforcement climate to fatal incidents involving federal agents during immigration operations in the Minneapolis Saint Paul area in January 2026, which fan organizations cited when raising concerns about police militarization around the tournament.

> **Cyber relevance:** Civil unrest, protest activity, and contentious immigration enforcement create fertile ground for disinformation and incitement campaigns, targeted harassment/doxxing of officials and activists, and opportunistic hacktivist messaging operations that piggyback on real grievances, a pattern explicitly anticipated in U.S. and FIFA intelligence briefings reported in March 2026, which flagged elevated potential for extremist attacks and civil unrest tied to immigration policy and the Iran conflict.

3.2 The U.S.–Iran Conflict and Iran's Tournament Exit

Since a military and cyber escalation between the United States/Israel and Iran began around late February 2026, referenced in Iranian aligned messaging as “Operation Epic Fury” and “Roaring Lion” Iran nexus threat actors have sharply increased claimed cyber operations against U.S. targets, including a med tech company, county government systems, a senior FBI official, and U.S. Marine Corps personnel. This conflict directly shaped Iran's World Cup experience: the Trump administration publicly questioned whether Iran should compete on U.S. soil; Iranian federation officials were barred from entering Canada for FIFA's April Congress over alleged IRGC ties; the Iranian squad relocated its base camp to Tijuana, Mexico, commuting across the border for matches rather than lodging in the United States; several team support staff (including the federation president) were denied U.S. visas; and Iran's ticket allocation was reportedly withdrawn shortly before its opening match.

Iran's captain and head coach publicly described the team as being treated unfairly and “oppressed,” and protests occurred outside at least one Iran match. Iran was eliminated from the tournament on June 27-28, finishing third in its group after three draws and narrowly missing one of the eight available third place qualification slots, extending the team's record to seven World Cup appearances without a knockout stage win.

> **Cyber relevance:** Iran linked groups (Handala Hack Team/Void Manticore, CyberAv3ngers, and a coalition of newer personas, DieNet, APTIran, Cyber Toufan, Cyber Support Front, Iranian Avenger, and Cyb3r Drag0nz, operating since late February 2026 under the banner of an “Electronic Operations Room of the Islamic Resistance Axis”) have an active grievance narrative, demonstrated intent, and recent operational tempo against U.S. targets. Iran's elimination removes any incentive to avoid disrupting matches the team itself is playing in, while the team's public complaints provide ready made justification for retaliatory action against the U.S. host nation generally, historically how these personas have framed disruptive or destructive operations.

3.3 Russia Ukraine War and NATO Tensions

Russia's national team remains suspended from FIFA and UEFA competition over the invasion of Ukraine and did not qualify for or participate in the 2026 World Cup. That absence from the pitch has not reduced the activity of Russia aligned cyber actors, whose targeting is driven by the broader war and NATO confrontation rather than football results. Russian state sponsored units have the most extensive track record of any nation state actor against major sporting events: the GRU's Sandworm unit (APT44/Unit 74455) deployed the destructive “Olympic Destroyer” wiper against the 2018 PyeongChang Winter Olympics opening ceremony, complete with false flag code designed to implicate other states, and APT28 (Fancy Bear) leaked stolen athlete medical records from the World Anti Doping Agency following the 2016 Rio Olympics. Russia linked actors were also reported targeting the Italian embassy in Washington, D.C. and Olympic adjacent hotels and venues during the 2026 Milan Cortina Winter Games.

The pro Russian hacktivist collective NoName057(16) is assessed as the most operationally consistent non state actor relevant to this tournament. It runs a crowdsourced “DDoSia” botnet with a point and reward incentive structure that blurs the line between ideological volunteers and

paid participants, and it has a recent history of targeting UK and other Western local government websites, as well as DDoS activity against the Milan Cortina Winter Olympics earlier in 2026. Cyber Army of Russia Reborn and various KillNet affiliated successors round out the pro Russian hacktivist ecosystem most likely to claim opportunistic activity tied to the World Cup.

3.4 U.S. China Strategic Rivalry

China remains the United States' primary geopolitical rival, with relations defined by technology competition, tariff disputes, and tension over Taiwan. Despite this friction, threat intelligence assessments judge that Beijing is unlikely to sponsor disruptive cyberattacks against the World Cup itself, disrupting a major event on U.S. soil would represent a significant escalation against a government that has shown a willingness to publicly attribute and sanction Chinese state linked operators. Instead, Chinese state tasked groups (including actors affiliated with or commercially tasked by the Ministry of State Security, and PLA aligned units) are assessed as likely to pursue opportunistic intelligence collection against selected attendees, delegations, and organizations consistent with Beijing's documented preference for long horizon espionage over disruption. A Chinese state linked group tracked as TAG-51/BlackTech previously compromised a telecommunications provider supporting the 2022 Qatar World Cup, illustrating the precedent for telecom sector targeting at this type of event. Separately, financially motivated Chinese cybercriminal infrastructure has cloned FIFA's website across roughly 300 domains to harvest fan data, a criminal rather than state directed activity.

3.5 Mexico: Organized Crime and Civil Unrest

Cartel and organized crime activity poses the most acute physical security risk among the three host nations, even though it is largely distinct from core cyber threats. A U.S. assisted Mexican operation that killed cartel leader “El Mencho” in February 2026 triggered retaliatory arson and vehicle attacks by organized crime groups in Guadalajara, disrupting tourism near a host stadium in the weeks before the tournament. Separately, protests over housing, water, transport, and electricity shortages greeted the reopening of Mexico City's renamed Banorte Stadium (formerly Estadio Azteca), which hosted the opening match. Reporting indicates no comparable safety concerns have emerged around Canadian host cities.

> **Cyber relevance:** Transnational criminal organizations operating in Mexico add to the country's baseline cybercrime risk profile (alongside opportunistic theft), and civil unrest of this kind creates the same disinformation amplification dynamic seen around U.S. immigration protests, a vector for hacktivist or troll farm messaging operations to exploit rather than create the underlying grievance.

3.6 Human Rights Criticism and Boycott Movements

Independent human rights organizations, including Amnesty International and Human Rights Watch, have characterized conditions in the United States as a human rights concern in the tournament context, citing immigration and border policy, restrictions on speech and assembly, and discrimination against LGBTQ+ communities; Human Rights Watch reported that nearly all U.S. host city committees had failed to produce adequate human rights action plans. These

criticisms, combined with the travel ban controversy, have fueled boycott petitions and public calls for a boycott from political and sporting figures in multiple European countries, adding a sustained reputational and information operations dimension to the tournament that hacktivist groups on multiple sides of the geopolitical spectrum have incentive to amplify.

4. Threat Actor Landscape

The actors relevant to the World Cup fall into three broad, sometimes overlapping categories: nation state directed groups pursuing espionage or disruption in support of strategic objectives; hacktivist and state aligned personas conducting lower cost symbolic or harassment operations, often with looser command and control than formal state units; and financially motivated cybercriminal groups, including ransomware operators, exploiting the event's visibility and transaction volume for profit. Defenders should not assume a clean separation between categories, several hacktivist collectives share botnets, access brokers, and infrastructure with profit driven cybercriminal ecosystems.

4.1 Nation State Directed Actors

Nation	Actor(s)	Assessed Role / Precedent
Russia	Sandworm / APT44 (GRU Unit 74455); APT28 / Fancy Bear	Deployed the destructive Olympic Destroyer wiper against the 2018 PyeongChang opening ceremony (DOJ indicted in 2020) and leaked WADA athlete medical data after the 2016 Rio Olympics; also linked to recent targeting of an embassy and venues around the 2026 Winter Olympics. Highest historical precedent for disruptive action against a major sporting event.
Iran	MOIS linked Handala Hack Team (aka Void Manticore / TAG-145 / Red Sandstorm / Banished Kitten); IRGC linked CyberAv3ngers (aka Bauxite / Hydro Kitten / Storm-0784 / UNC5691); GreenHotel (Cotton Sandstorm / Emennet Pasargad); GreenBravo (APT42 / Charming Kitten / Mint Sandstorm)	Active wartime posture against U.S. targets since February 2026, including a confirmed destructive wiper attack on a U.S. medical technology firm in March 2026. CyberAv3ngers has a documented history of compromising internet exposed industrial control systems at U.S. water utilities. No confirmed campaign against core World Cup infrastructure identified to date, but capability and intent against U.S. public/private networks are both established.
China	MSS and PLA affiliated espionage units; TAG-51/BlackTech; Volt Typhoon	Long horizon intelligence collection against delegations, executives, and officials assessed as likely; disruptive action against the tournament itself assessed as unlikely given escalation risk. BlackTech

Nation	Actor(s)	Assessed Role / Precedent
		previously compromised a telecom provider supporting the 2022 Qatar World Cup.

4.2 Hacktivist and State Aligned Personas

Group	Profile
NoName057(16)	The most operationally consistent pro Russian hacktivist group active in 2026; runs the crowdsourced “DDoSia” DDoS botnet with a paid/point based incentive model; recent targeting of UK and other Western local government websites and the 2026 Winter Olympics.
Handala Hack Team	Iran aligned (MOIS/Void Manticore-linked) persona; claimed responsibility for a March 2026 destructive wiper attack on a U.S. med-tech firm and for numerous claims against U.S. government and defense adjacent targets since February 2026, including an unverified claim of breaching an FBI drone surveillance network around World Cup security operations; known pattern of exaggerated impact claims that warrant skepticism.
CyberAv3ngers	IRGC Cyber Electronic Command's industrial control system specialist unit; previously compromised dozens of internet exposed water utility control devices across the U.S., including a 2023-24 incident at a Pennsylvania municipal water authority; municipal water/energy systems in World Cup host cities sit squarely within its documented targeting profile.
Electronic Operations Room of the Islamic Resistance Axis (and affiliated personas DieNet, APTIran, Cyber Toufan, Cyber Support Front, Iranian Avenger, Cyb3r Drag0nz)	A coalition of Iran aligned personas formed in late February 2026 amid the U.S. Iran escalation, has claimed DDoS attacks against Gulf state airports and banks, illustrating intent and capability against transportation and finance sector targets directly relevant to fan facing infrastructure.
Cyber Army of Russia Reborn / KillNet-affiliated successors	Pro Russian hacktivist clusters with a history of opportunistic DDoS and defacement campaigns against Western government and infrastructure targets, generally operating independent of any single triggering event.

4.3 Financially Motivated Cybercriminal and Ransomware Groups

Group(s)	Relevance
Qilin, DragonForce, Akira, Play, ALPHV/BlackCat affiliates	Active ransomware operations capable of targeting hospitality providers, vendors, and other organizations whose continuous availability is essential during the tournament window; a comparable precedent occurred in 2024 when Italy's Bologna Football Club suffered a 200GB data theft and ransom incident affecting player, financial, and stadium data.
Scattered Spider / Muddled Libra; Silent Ransom Group	Social engineering driven intrusion crews known for help desk impersonation and credential based access to corporate environments; relevant to the large temporary vendor and sponsor ecosystem supporting the tournament.
Diffuse cybercrime ecosystem (ticket fraud, fake job/HR sites, romance-and-rental scams, AI-enhanced phishing)	The highest volume threat category by incident count. Tens of thousands of FIFA themed domains have been registered since January 2026, with a meaningful share confirmed malicious, fraud spans counterfeit ticketing, fake employment and volunteer postings (including a weaponized “employee handbook” PDF used against host-city staff), fraudulent short term rentals, rideshare/transport scams, fake livestream apps, counterfeit merchandise, and fraudulent cryptocurrency tokens impersonating players.

5. Threats Observed Leading Up to the First Match (January-June 11, 2026)

Threat actors did not wait for kickoff. Multiple independent research teams reported that cybercriminal infrastructure was “staged and waiting” months in advance of the opening match, with malicious activity scaling steadily from January 2026 onward.

5.1 Domain Registration and Brand Impersonation

- Researchers identified more than 13,000 new FIFA World Cup themed domains registered between January and May 2026, roughly 8.8% of which were assessed malicious or suspicious.
- Researchers also separately tracked approximately 19,000 “fifa” themed domains created since January 2026; a Cyber Intelligence Center identified more than 4,300 fake FIFA domains alongside upward of 1.5 million compromised accounts and over 7,300 leaked credentials linked to the tournament's digital ecosystem.
- Chinese cybercriminal operators were reported to have cloned the official FIFA website across roughly 300 domains specifically to harvest fan data.
- The FBI's Internet Crime Complaint Center (IC3) issued a public service announcement in May 2026 warning of a surge in spoofed FIFA websites using typo squatting and alternate top level domains, and separately warned in May of spoofing attacks targeting the official FIFA website itself.

5.2 Targeting of Organizers and Host City Staff

- Researchers identified fake career sites built to harvest Google Workspace credentials from job seekers, and a weaponized “employee handbook” PDF used to target staff at one host city.
- Researchers also characterized the campaign as high volume phishing using the World Cup as cover, aimed at both fans and the organizations supporting the event, with lures delivered via Discord, WhatsApp, and Telegram.

5.3 Government Preparedness Activity

- CISA conducted cyber and physical vulnerability assessments at 10 of the 16 host stadiums, plus FIFA base camps, hotels, and related critical infrastructure, including six dedicated exercises in January 2026 alone.
- Canada's federal provincial territorial framework and the Canadian Centre for Cyber Security engaged host cities and infrastructure operators on incident response coordination.
- Mexico's Secretariat of Security and Citizen Protection (SSPC) issued early alerts on cyber enabled fraud targeting ticketing, travel, and accommodation services as early as March 2026.

5.4 A Wartime Precedent: The Stryker Incident

On March 11, 2026, the Handala Hack Team (linked to Iran's Ministry of Intelligence and Security) executed a destructive wiper attack against U.S. medical technology company Stryker, abusing the company's own Microsoft Intune mobile device management platform to push the malicious payload. While unrelated to the World Cup directly, the incident is the clearest demonstration to date of Iran aligned willingness and capability to conduct destructive operations against U.S. commercial targets during the current conflict, and it establishes a credible technical precedent (abuse of legitimate enterprise management tools) that could be repurposed against any of the many vendors supporting the tournament.

6. Threats Observed During the Tournament (June 11-June 28, 2026)

Since the opening match, reporting confirms that the pre tournament threat patterns have continued and, in some categories, intensified, while no confirmed destructive attack against core tournament infrastructure has been publicly attributed as of this writing.

6.1 Confirmed and Reported Cyber Activity

- Multiple regional ticketing portals have experienced service outages attributed to coordinated distributed denial of service (DDoS) attacks, with some incidents claimed by hacktivist groups on Telegram and X (formerly Twitter); these claims are generally unverified by independent researchers.
- Phishing, credential harvesting, and fraudulent ticketing activity has continued at high volume throughout the group stage, consistent with the pre tournament build up.
- The Handala Hack Team publicly claimed to have breached an FBI drone surveillance network allegedly used to monitor World Cup venues, asserting access to facial recognition data and vehicle tracking information. This claim has not been independently verified and is consistent with the group's documented pattern of exaggerating operational impact for propaganda value; it should be treated as an influence operation data point rather than a confirmed compromise.
- Researchers continue to observe circulation of malware families historically associated with prior destructive and credential theft campaigns (including code linked to past Olympic Destroyer, HermeticWiper, RedLine infostealer, and BlackCat/ALPHV activity) in the general threat environment surrounding the tournament; their presence indicates a diverse and active threat landscape rather than confirmed targeting of World Cup systems specifically.

6.2 Civil Unrest and Physical-Digital Convergence

- Protests occurred outside at least one Iran match amid the team's visa and travel disputes, reportedly prompting U.S. officials to order the Iranian delegation back to its Tijuana training base ahead of schedule.
- ICE's stadium presence and continued visa enforcement (including the Ghana/Canada visa denial and earlier Iraq and Somalia incidents) have sustained an elevated protest and labor action environment in and around several U.S. and Canadian venues.
- FIFA has stated it is not involved in host government visa adjudication and that admission decisions rest with each host nation a position that has drawn criticism from players, federations, and rights organizations but leaves the underlying enforcement dynamic, and its associated unrest, unresolved for the remainder of the tournament.

> **Assessment:** No confirmed, independently verified disruptive cyberattack against core World Cup infrastructure (ticketing backbone, stadium operations technology, or broadcast systems) has occurred through the group stage. The dominant confirmed activity remains financially motivated cybercrime and opportunistic DDoS against secondary/regional systems. Hacktivist

> claims of more significant access (e.g., the FBI drone network claim) remain unverified and should be weighted accordingly, though they still carry reputational and disinformation value for the actors making them.

7. Sector by Sector Cyber Risk Assessment

The World Cup's digital ecosystem extends far beyond FIFA's own systems into nearly every sector operating in or near a host city. The following assessment covers the sectors most frequently identified in current threat reporting.

7.1 Critical Infrastructure Water, Wastewater, and Energy

This is the highest impact, if not highest likelihood, sector at risk. CyberAv3ngers' documented escalation curve against internet exposed industrial control systems is the single most important data point for defenders of municipal infrastructure in U.S. host cities. A 2024 CISA assessment found that over 70% of inspected U.S. water utilities were non compliant with Safe Drinking Water Act cybersecurity requirements, commonly citing default passwords and shared logins. Precedent incidents include the 2023-24 compromise of a Pennsylvania municipal water authority's control interface (left with a pro Iran message) and a January 2024 Russian linked attack that caused a Texas municipality's water tank to overflow after earlier attempts against neighboring systems failed. Ransomware attacks against water sector targets have also occurred independent of this conflict.

7.2 Transportation

Transit systems, rideshare platforms, and airport/border adjacent infrastructure face both fraud and disruption risk. Iran aligned personas operating under the “Electronic Operations Room of the Islamic Resistance Axis” banner have already claimed DDoS attacks against Gulf region airports, illustrating intent against transportation targets generally. QR code fraud is described as the fastest growing fraud variant tied to the tournament, with fake shuttle passes, parking permits, and fan transport QR codes identified as a high risk vector given the geographic spread of the 16 city footprint; rideshare related scams have also been observed.

7.3 Telecommunications

Millions of visitors using mobile networks simultaneously in host cities create both capacity strain and an attractive target for signaling protocol exploitation, service disruption, or communications interception. China linked group TAG-51/BlackTech previously compromised a telecommunications provider supporting the 2022 Qatar World Cup, demonstrating precedent for telecom sector targeting at this category of event; Volt Typhoon's broader, separately documented pre positioning inside U.S. critical infrastructure (including telecom adjacent systems) adds to the sector's exposure independent of the tournament.

7.4 Financial Services

Payment processors and identity providers underpinning ticketing, hospitality, and merchandising face fraud at scale: fraudulent payment capture via fake checkout pages, business email compromise against vendors and sponsors, fraudulent cryptocurrency tokens impersonating players, and sports betting manipulation schemes have all been reported. The compressed, high volume, cross border transaction environment of the tournament unfamiliar

merchants, fast international payments, limited scrutiny, is repeatedly cited by analysts as structurally favorable to financial cybercrime.

7.5 Hospitality and Travel

Hotels, short term rental platforms, and digital key/point of sale systems are exposed to ransomware (Qilin, DragonForce, Akira, Play, and ALPHV/BlackCat affiliates are the groups most frequently named in current reporting), alongside fraudulent rental listings, demands for off platform wire transfers or cryptocurrency payment, and identity provider compromise. Researchers have specifically warned fans to avoid off platform payment requests and to use credit cards with chargeback protection rather than wire transfers or cryptocurrency when booking accommodation.

7.6 Healthcare and Medical Technology

While not a primary tournament support sector, the March 2026 Handala wiper attack against medical technology firm Stryker demonstrates that Iran aligned a ctors are actively targeting U.S. healthcare adjacent technology providers during the current conflict window, via abuse of legitimate device management platforms. Any medical technology or health services vendor supporting team medical staff, stadium first aid, or hostcity emergency response should be considered within the indirect blast radius of this threat pattern.

7.7 Government and Municipal Services

Pro Russian hacktivist DDoS (principally NoName057(16)) has repeatedly demonstrated the ability to take state and local government websites offline for hours, with documented recent targeting of UK local government services; CISA names “government services and facilities, including local municipalities” as one of three sectors explicitly called out in connection with the active Iran nexus industrial control, system campaign. Host city governments also sit at the center of the immigration enforcement controversy, making their public facing websites and communications channels plausible targets for both DDoS and disinformation/defacement seeking to amplify the political narrative around ICE activity.

7.8 Media and Broadcasting

Streaming platforms and broadcasters are high value DDoS targets precisely because disruption during a live, high viewership match generates outsized reputational and political impact. DDoS attacks successfully disrupted online broadcasts of host nation matches during UEFA Euro 2024 (targeting Poland's coverage), and the 2018 Olympic Destroyer wiper disrupted the PyeongChang opening ceremony's Wi-Fi, ticketing systems, official app, and event website simultaneously, the standing benchmark case for what a determined nation state actor can achieve against this category of target. Fraudulent livestreaming apps bundled with malware, and unauthorized IPTV services, represent the consumer facing extension of this risk.

8. Mapping Geopolitical Flashpoints to the Remaining Bracket

As of June 28, 2026, the group stage is complete and the Round of 32 is under way (through July 3), followed by the Round of 16 (July 4–7), Quarterfinals, Semifinals, the Third Place Playoff (July 18, Hard Rock Stadium, Miami Gardens), and the Final (July 19, MetLife Stadium, East Rutherford, New Jersey). From the Round of 16 onward, every remaining match is played exclusively in the United States, which concentrates the remaining window of geopolitical cyber risk onto U.S. soil specifically, even though Mexico and Canada's group stage and early knockout hosting duties are now largely complete.

8.1 Iran's Exit: A Risk That Outlives the Bracket

Iran's elimination on June 27-28 means no remaining fixture carries direct Iran vs host nation symbolism on the pitch. This is unlikely to reduce Iran aligned cyber activity, for three reasons: first, Iran nexus targeting of the United States is driven by the broader military conflict, not by the football tournament, and will continue on its own timeline; second, the Iranian team and federation's public framing of their tournament experience as discriminatory provides exactly the kind of grievance narrative that Handala and CyberAv3ngers have previously used to justify retaliatory messaging operations against the U.S. “host,” independent of which teams remain in the competition; and third, removing Iran from the spotlight of match coverage may paradoxically free these personas to act without the scrutiny that comes from being associated with an active participant, while still invoking the tournament's name for visibility.

8.2 The Host Nation's Own Run

The United States advanced from the group stage and faces Bosnia and Herzegovina in the Round of 32 (July 1, Levi's Stadium, San Francisco Bay Area), with a potential Round of 16 meeting against the winner of Belgium vs. Senegal. As the most symbolically significant team for hacktivist messaging purposes, representing the host nation whose immigration and foreign policy are already contested, any U.S. match is assessed as carrying disproportionate hacktivist interest relative to its sporting stakes alone, particularly given that several U.S. matches are scheduled in sanctuary city markets where ICE related tension is highest.

8.3 Sanctuary-City Venues in the Closing Rounds

Seven of the eleven U.S. host cities, including Boston, Los Angeles, the New York/New Jersey metro area, Philadelphia, Seattle, and the San Francisco Bay Area, are sanctuary jurisdictions that the Department of Homeland Security has suggested could face disrupted customs processing if local authorities continue declining to cooperate with federal immigration enforcement. Several of these cities (Los Angeles/SoFi Stadium, the Bay Area, Seattle, Philadelphia, and the New York/New Jersey area) continue hosting matches throughout the knockout rounds, meaning the immigration enforcement flashpoint and its associated protest, labor, and disinformation activity will remain active in parallel with the highest stakes football of the tournament rather than fading as the bracket narrows.

8.4 The Final: Single Highest Value Target Window

The July 19 final at MetLife Stadium represents the tournament's point of maximum concentration: the largest expected security footprint, the highest density of visiting dignitaries and government delegations (maximizing espionage value for Russian, Chinese, and Iranian intelligence services), the single largest global broadcast audience (maximizing the propaganda value of any successful DDoS or defacement against streaming/broadcast infrastructure), and the clearest historical analogue to the 2018 PyeongChang opening ceremony wiper attack in terms of symbolic timing. Physical security planning has already flagged drone activity as a complicating threat at outdoor venues and fan zones during high profile windows, with FAA flight restrictions and FEMA funded counter drone mitigation specifically referenced in tournament security preparations; this physical threat increasingly overlaps with cyber response, since drone detection and mitigation rely on networked sensors and command center systems that are themselves potential targets.

8.5 Russia and China: Independent of the Bracket

Because Russia is not competing and China linked activity is assessed as primarily espionage-driven, neither nation's cyber posture is expected to track specific match outcomes. Pro Russian hacktivist DDoS activity (NoName057(16) and successor KillNet affiliated groups) will most plausibly continue at a steady opportunistic tempo tied to the broader Ukraine conflict and NATO related news cycles, with the tournament serving as a target rich, high visibility backdrop rather than the proximate cause of any single incident.

9. Predictive Outlook for the Remainder of the Tournament (June 28-July 19, 2026)

The following forecast uses standard likelihood language (consistent with intelligence-community tradecraft: “almost certain,” “likely,” “even chance,” “unlikely,” “remote”) to characterize each threat category through the close of the tournament.

Threat Category	Likelihood	Potential Impact	Forecast Note
Phishing, credential theft, and fraudulent ticketing/hospitality sites	**High**	**Medium**	Almost certain to continue at or above current volume through the final; will likely spike again around Round of 16 and Final ticket resale activity.
DDoS against ticketing, streaming, or host city government websites	**High**	**Medium**	Likely to recur multiple times before July 19, most plausibly timed to high-viewership matches (USA, Brazil, Argentina, England, host nation fixtures) or in response to unrelated geopolitical news.
Ransomware against hospitality, vendor, or sponsor organizations	**Medium-High**	**High**	An even chance of at least one publicly disclosed incident before the tournament ends, given the size of the temporary vendor ecosystem and precedent (Bologna FC, 2024).
Hacktivist defacement / leak / harassment campaign tied to Iran or immigration narrative	**Medium-High**	**Medium**	Likely, particularly around U.S. host nation matches and sanctuary city venues; impact expected to be reputational/disinformation-focused rather than operationally disruptive.
Destructive wiper or ICS attack against host city critical infrastructure (water/energy)	**Low**	**Very High**	Remains a low probability, high consequence scenario. Capability and intent exist (CyberAv3ngers, Sandworm precedent) but no corroborated indicators of an active campaign

Threat Category	Likelihood	Potential Impact	Forecast Note
			against World Cup linked infrastructure specifically have been identified.
State espionage against delegations, athletes, or officials	**High**	**Medium**	Almost certainly ongoing continuously; unlikely to be publicly attributed in real time given the low visibility nature of intelligence collection.
AI generated disinformation, deepfakes, or synthetic media incidents	**Medium**	**Medium**	Likely to increase around marquee knockout matches and the final, including impersonation of athletes/officials and fabricated security incident reports designed to cause confusion or strain public resources.
Civil unrest / protest activity intersecting with online incitement near venues	**Medium**	**Medium**	Likely to persist in sanctuary city host markets through the closing rounds, tracking immigration-enforcement activity rather than match results.
Drone incursions at outdoor venues/fan zones with cyber-physical overlap	**Medium**	**Medium**	Likely to recur at high-attendance outdoor events, particularly the final; risk is primarily physical security but intersects with networked detection/command systems.

Bottom line: The most probable outcome through July 19 is a continuation of the current pattern, high volume, low individual severity financial cybercrime as the dominant activity, punctuated by intermittent, opportunistic, and largely symbolic hacktivist DDoS or defacement incidents tied to the Iran conflict, the Russia Ukraine war, or U.S. immigration policy. A single catastrophic, infrastructure disabling event remains possible but is not the most likely scenario based on currently available indicators; risk is highest around marquee host nation matches, sanctuary city venues, and the July 19 final.

10. Recommendation

10.1 For Tournament Organizers, Host Cities, and Critical-Infrastructure Operators

- Maintain (or stand up where absent) a joint, multi jurisdictional cyber operations center linking CISA, the Canadian Centre for Cyber Security, Mexico's CERT MX/SSPC, the FBI, and the RCMP, with clear escalation paths across all three legal jurisdictions.
- Complete credential rotation, default password, and remote access audits across every municipal water, wastewater, and energy system in or near a host city, prioritizing internet-exposed industrial control system interfaces.
- Run DDoS, ransomware, and disinformation tabletop exercises specifically timed before each remaining high profile match window (Round of 16, Quarterfinals, Semifinals, Final), rather than relying solely on pre tournament preparation.
- Inventory the full vendor and supplier graph for each remaining host city, with particular attention to ticketing, hospitality, and payment processing vendors that have not yet been independently security tested.
- Pre stage public communications templates for rumor control, given the demonstrated risk of AI generated disinformation about security incidents during marquee matches.

10.2 For Sponsors, Vendors, and Broadcasters

- Treat brand protection and takedown operations against fraudulent domains, fake job postings, and counterfeit ticketing sites as an ongoing operational function through July 19, not a pre tournament task that is now complete.
- Validate multi factor authentication, password reset, and ticket transfer/resale logic against credential stuffing and account takeover attempts, given the millions of already leaked credentials circulating in connection with the tournament.
- Confirm CDN and DDoS mitigation capacity, status pages, and incident contacts are current ahead of each remaining high viewership broadcast window.

10.3 For Fans, Media, and Travelers

- Purchase tickets, merchandise, and hospitality packages only through FIFA's official platforms; treat off platform wire transfers or cryptocurrency requests as an immediate red flag, and use a credit card with chargeback protection for all purchases.
- Avoid sideloading World Cup related mobile applications and verify any app against FIFA's official published list before downloading; stream matches only through licensed platforms rather than third party sites or Telegram links.
- Be cautious with public QR codes at venues, viewing parties, and informal transport/parking arrangements; verify codes against official signage where possible.

- Travelers, particularly those from one of the 39 countries affected by current U.S. travel restrictions, should review the published civil society travel advisories, confirm visa status well in advance, and have a contingency plan for potential delays or denial of entry.
- Keep mobile devices patched, use a reputable VPN or cellular data rather than open public Wi-Fi where possible, and disable automatic Wi-Fi network joining while at venues or fan zones.

11. Sources Consulted

This section lists the publicly available reporting and analysis drawn on between approximately January and June 28, 2026, and assesses each source using the NATO Admiralty Code. Under that code, the letter score (A to F) rates source reliability and is assessed independently of the digit score (1 to 6), which rates the credibility of the specific information used. A B2 rating, for example, denotes a usually reliable source reporting information assessed as probably true. Ratings reflect this analyst's assessment at the time of writing rather than any self rating by the source organisations, and apply to the use made of each source in this report, not to that source in general. This report does not reproduce any source's text verbatim; all analysis above reflects independent synthesis.

11.1 Scale Legend

Code	Source Reliability	Code	Information Credibility
A	Completely reliable	**1**	Confirmed by other sources
B	Usually reliable	**2**	Probably true
C	Fairly reliable	**3**	Possibly true
D	Not usually reliable	**4**	Doubtfully true
E	Unreliable	**5**	Improbable
F	Reliability cannot be judged	**6**	Truth cannot be judged

11.2 Source Evaluation Matrix

Source	Type	Rel.	Cred.	Use in this report	Rationale
Cybersecurity authorities					
CISA (U.S. Cybersecurity and Infrastructure Security Agency)	Government CERT	**A**	**2**	ICS and water sector risk, federal preparedness posture	Authoritative national CERT; advisories corroborated by Canadian Centre and FBI IC3.

Source	Type	Rel.	Cred.	Use in this report	Rationale
Canadian Centre for Cyber Security	Government CERT	**A**	**2**	Tri-national coordination context	National authority; aligned with CISA reporting on shared threat actors.
FBI Internet Crime Complaint Center (IC3)	Federal law enforcement	**A**	**2**	Cybercrime and fraudulent ticketing trend data	Federal reporting on cybercrime; corroborated by CISA advisories and trade press.
Mexico SSPC (Secretariat of Security and Citizen Protection)	Government	**B**	**2**	Mexican host city context, organised crime overlap	National security authority; less corroboration in English-language sources.
Threat intelligence vendors					
Recorded Future / Insikt Group	Commercial TI	**B**	**2**	Threat actor attribution, brand impersonation tracking	Strong attribution track record; cross-checked against peer vendors.
Unit 42 (Palo Alto Networks)	Commercial TI	**B**	**2**	Ransomware ecosystem and espionage activity	Sound primary research; vendor publication incentive acknowledged.
KELA Cyber	Commercial TI	**B**	**2**	Underground market and credential leak tracking	Specialist in dark web monitoring; corroborated against Flashpoint and Intel 471.
Flashpoint	Commercial TI	**B**	**2**	Threat actor forums and leak site monitoring	Established vendor with deep web and criminal forum coverage.
FortiGuard Labs (Fortinet)	Commercial TI	**B**	**2**	Telemetry-driven trend reporting	Telemetry-based reporting; attribution claims cross-referenced before reliance.
Arctic Wolf	Commercial TI	**B**	**2**	Incident response trend insights	MDR vendor with regular incident reporting; corroborated against industry.

Source	Type	Rel.	Cred.	Use in this report	Rationale
Intel 471	Commercial TI	**B**	**2**	Cybercriminal underground intelligence	Strong specialist niche; corroborated against KELA and Flashpoint.
SOCRadar	Commercial TI	**B**	**3**	Threat surface and exposure monitoring	Useful coverage; some marketing-influenced framing flagged.
CYFIRMA	Commercial TI	**B**	**3**	Supplementary regional context	Less established Western track record; treated as supporting rather than primary.
PolySwarm	Commercial TI	**B**	**3**	Malware detection telemetry	Emerging vendor; supporting role; corroborated where load-bearing.
Rescana	Commercial TI	**B**	**3**	Supplementary attack surface context	Smaller vendor; used for breadth only, not primary attribution.
Crisis24	Risk intelligence	**B**	**2**	Physical and geopolitical risk convergence analysis	Strong physical security and geopolitical risk reporting; relevant to cyber-physical overlap.
Trade and technology press					
Dark Reading	Trade press	**C**	**2**	Industry coverage and vendor disclosure tracking	Established cybersecurity publication; secondary reporting, not primary attribution.
Cybersecurity Dive	Trade press	**C**	**2**	Industry coverage, incident reporting	Editorial process intact; useful for breadth, not primary attribution.
Computer Weekly	Trade press	**C**	**2**	Industry coverage, UK and international	Long-established trade title; secondary reporting.

Source	Type	Rel.	Cred.	Use in this report	Rationale
Insurance Times	Trade press	**C**	**3**	Cyber insurance market context	Limited cyber-specific expertise; used for insurance sector framing only.
Policy institutes and advocacy organisations					
Center for Strategic and International Studies (CSIS)	Policy institute	**B**	**2**	Geopolitical context, Iran, Russia, China posture	Strong analytical reputation; assessments rather than incident reporting.
Council on Foreign Relations (CFR)	Policy institute	**B**	**2**	Foreign policy framing of state-aligned threats	Strong analytical reputation; cross-referenced with other policy sources.
American Civil Liberties Union (ACLU)	Rights organisation	**C**	**2**	Civil rights and immigration enforcement impacts	Stated advocacy position; factual claims corroborated by news reporting.
American Immigration Council	Rights organisation	**C**	**2**	Immigration enforcement data and analysis	Advocacy organisation; statistical claims cross-checked with government reporting.
News organisations					
NPR	Mainstream news	**B**	**2**	U.S. domestic and geopolitical coverage	Public broadcaster with established editorial standards.
Al Jazeera	Mainstream news	**B**	**2**	Iran, Middle East, and global South perspective	Editorial process intact; useful counterweight to Western framing.
Reuters (via secondary citation)	Newswire	**B**	**2**	Geopolitical events and immigration enforcement reporting	Internationally respected newswire; some claims accessed via secondary citation.
Yahoo Sports	Sports media	**C**	**2**	Fixtures and match scheduling	Factual sports reporting; non-cyber context only.

Source	Type	Rel.	Cred.	Use in this report	Rationale
ESPN	Sports media	**C**	**2**	Fixtures and match scheduling	Factual sports reporting; non-cyber context only.
CBS Sports	Sports media	**C**	**2**	Fixtures and match scheduling	Factual sports reporting; non-cyber context only.
Sky Sports	Sports media	**C**	**2**	Fixtures and match scheduling	Factual sports reporting; non-cyber context only.
Wikipedia (FIFA 2026 schedule and controversy pages)	Crowd-sourced reference	**F**	**3**	Schedule and controversy tracking	Reliability cannot be independently assessed; used only where corroborated by primary sources.

11.3 Corroboration and Single-Source Claims

No load bearing judgment in this report rests on a single source rated below B2. Critical infrastructure risk assessments (Section 7.1) draw on CISA, the Canadian Centre for Cyber Security, and at least one commercial TI vendor rated B2 or higher. Threat actor attribution claims (Section 4) are corroborated across at least two commercial TI vendors or one government CERT plus one commercial vendor. Geopolitical context (Sections 3.1 to 3.6) is corroborated across at least two of mainstream news, policy institute, and commercial TI reporting. Sources rated B3 or C3 are used only for breadth or as supporting context, never as the sole basis for a key judgment.

11.4 Confidence Statement

The overall source mix is weighted toward government CERTs and established commercial threat intelligence vendors, with trade press and advocacy reporting in a supporting role. On this basis, the High confidence judgments in Section 1 (Key Judgments) rest on multiple B2 or higher sources across at least two source categories; the Moderate confidence judgments rest on at least two corroborating sources of mixed type; and the Low confidence forward looking forecasts in Section 9 reflect analytic judgment informed by, but not solely derived from, the source set above. Confidence levels should be re examined if any cited source materially revises its assessment between now and the 19 July final.

This document is a point in time situational awareness synthesis as of June 28, 2026. Given the pace of both the tournament and the underlying geopolitical conflicts described above, readers should treat all forward looking assess as provisional and seek updated reporting from the cited sources as the knockout rounds progress toward the July 19 final.