

# Security Lessons from the Paris Olympics for the 2026 FIFA World Cup and Other Major Events

By Alexandre Rodde, David Mcilhatton, John Cuddihy, and Shannen Benton

**This article examines how security lessons from the 2024 Paris Olympics can inform preparations for the 2026 FIFA World Cup taking place across the United States, Canada, and Mexico this summer. As the largest tournament in football history, the World Cup will present an unprecedented security challenge spanning 16 host cities, three countries, and millions of spectators. Paris demonstrated the value of intelligence-led counterterrorism, integrated multi-agency coordination, critical infrastructure protection, cybersecurity readiness, counter-drone capabilities, visible deterrence, and effective public communication. Despite a complex threat environment, the Games concluded without any major incidents, highlighting the effectiveness of preventive and adaptive security measures. Applying these lessons to a larger, multi-jurisdictional tournament will require exceptional cross-border cooperation, harmonized planning, and scalable responses to terrorism, crime, sabotage, cyber threats, and public disorder.**

**W**hen the 2026 FIFA World Cup begins across North America in June, it will represent the largest tournament in the history of international football. For the first time, the competition will involve teams from 48 countries and more than 100 matches hosted across 16 cities in three countries: the United States, Canada, and Mexico.<sup>1</sup> The scale of the tournament will be unprecedented, with millions of spectators expected to attend matches in person and billions more following the event on television and through digital media platforms.<sup>2</sup> For governments and security agencies, however, the tournament represents far more than a major event. Sporting events of this scale have long been viewed as attractive targets for threat actors to cause harm, as they draw large crowds, generate global media coverage, and often carry significant value for host nations. Because of this, even minor incidents before and during these events can attract global attention and cause widespread effects.<sup>3</sup>

A previous article published in *CTC Sentinel* in 2024 by some of the authors<sup>4</sup> examined in detail how terrorist actors have historically targeted or attempted to attack major sporting events around the world, highlighting the motivations, tactics, and vulnerabilities associated with such high-profile gatherings. Rather than revisiting those cases here, this article builds on that earlier analysis by drawing lessons from the security planning and operational experience of the 2024 Summer Olympics in Paris. In doing so, it considers how the terrorist threat environment surrounding major international events has continued to evolve, particularly in relation

to emerging risks such as hybrid threats, cyber-enabled disruption, and other related activities such as infrastructure sabotage. It also reflects on how public-facing communication and visitor behavior formed part of the preventive security posture in Paris and how similar approaches might be adapted for the 2026 World Cup.

## The 2024 Paris Olympics Threat Environment

The 2024 Paris Olympics took place from July 26 to August 11 without any major security incidents, despite significant concerns in the media and from security commentators regarding its organization and national security planning in the context of a complex and diverse threat landscape. The opening ceremony on the Seine River and the 17 days of competition were protected by an extensive security operation, the scale of which had never been seen before in France and which brought together law enforcement, defense, security, and intelligence agencies; other government departments; and the security teams of participating countries.

This relative success was against the backdrop of a complex threat environment that included state threats, terrorism and extremism, general crime, as well as cyber security challenges that were exacerbated by the geopolitical situation at the time. Although the most severe scenarios that had been anticipated prior to the Games ultimately did not occur, a number of security incidents in the lead-up to and during the event nevertheless drew considerable attention, highlighting the ongoing challenges faced by organizers and law enforcement in ensuring the safety of participants and spectators. These incidents are summarized below.

---

*Alexandre Rodde is a Visiting Fellow at the Protective Security Lab at Coventry University. He works as a security consultant and analyst, specializing in terrorism, mass shootings, and violent extremism in the French national security apparatus. He is the author of *Le Jihad en France: 2012-2022* (not yet available in English).*

*Professor David Mcilhatton is Associate Pro Vice Chancellor for Defence and National Security, and Director of the Protective Security Lab at Coventry University.*

*Professor John Cuddihy is a Visiting Professor in the Protective Security Lab at Coventry, a former Head of Counter Terrorism in Police Scotland, and a consultant for international organizations on counterterrorism.*

*Shannen Benton is the Head of External Research at the National Counter Terrorism Security Office (NaCTSO), part of Counter Terrorism Policing.*

© 2026 Rodde, Mcilhatton, Cuddihy, Benton



Security personnel look on outside Estadio Guadalajara on March 26, 2026, in Zapopan, Mexico, prior to a FIFA World Cup 2026 Qualifying Playoff tournament match. (Luis Cano/Jam Media/Getty Images)

### **Terrorism and Extremism**

As highlighted in the 2024 article “Protecting Major Sporting Events from Terrorism: Considerations for the Paris Olympics and Beyond,” jihadism had remained France’s principal terrorist threat over the preceding decade and was the focus of heightened scrutiny in the months leading up to the Games. Indeed, globally the jihadi threat, especially from the Islamic State, was particularly high. The network had conducted high-profile attacks in Moscow and Iran just prior to the Paris Olympics and had issued numerous threats specifically targeting the Games through different media sources.

According to the Parquet National Anti-Terroriste (PNAT)—France’s national terrorism prosecution office—three major plots were successfully disrupted prior to the Olympics, in the Saint-Étienne, Yvelines, and Gironde regions, resulting in the arrest of approximately 40 individuals.<sup>5</sup> In an effort to preempt potential attacks, French security services conducted 936 administrative searches targeting suspected individuals,<sup>a</sup> while more than 700 individuals were placed under *mesures individuelles de contrôle administratif de surveillance* (MICAS),<sup>6</sup> which prohibited them from leaving their registered municipalities and required daily reporting to local police authorities. The majority of those subject to MICAS measures were connected to a jihadi network, though individuals associated with violent far-left and far-right extremist groups were also included. Although a limited number of these administrative restrictions were subsequently contested in court,

the measures seem to have proven effective in mitigating potential threats and ensuring the security of participants and spectators throughout the duration of the Games.

In one incident, three masked and armed militants declaring themselves members of the *Front de libération nationale corse* (FLNC) made a highly unusual and provocative public intervention at the Ghjurnate Internazionale di Corti, an annual conference of Corsican autonomist and independence activists in Corte, France.<sup>7</sup> The group took to the stage immediately after a speech by the spokesperson of the contemporary Corsican nationalist party Nazione, with one of the militants reading from a four-page prepared statement.<sup>8</sup> Their speech criticized the rise of far-right politics in Europe, denounced extreme right-wing influence on Corsica, and reiterated longstanding FLNC demands for greater autonomy and recognition of Corsica’s status,<sup>9</sup> including calls for the island’s inclusion on a list of non-self-governing territories to be decolonized.

Shortly before the Games, French police arrested Abdelouahed El-Baghdadi, the brother-in-law of terrorist Mohammed Merah,<sup>10b</sup> near a fan zone in Vincennes, Val-de-Marne<sup>11</sup> in connection with violence against his roommate. He was listed on a *fiche S*,<sup>12</sup> which identifies individuals considered a potential threat to national security. Although he was unarmed and there was no evidence of a planned attack on the Olympic events, his arrest demonstrated

a Compared to 153 administrative searches in all of 2023. “Pas d’attentat pendant les Jeux de Paris 2024 : le procureur antiterroriste salue le défi relevé Europe 1,” AFP, September 11, 2024.

b French terrorist Mohammed Merah killed seven individuals in southwestern France in March 2012; he was subsequently killed in a police standoff. See Scott Sayare, “Suspect in French Killings Slain as Police Storm Apartment After 30-Hour Siege,” *New York Times*, March 22, 2012.

the vigilance of French authorities and the importance of close monitoring of known extremist actors in areas of high public concentration.

While not directed at the Games themselves, two suspected jihadi attacks did take place during the time span of the Games. At the Laon correctional center, an inmate armed himself with a broken bottle and attacked prison staff, injuring one guard before being restrained.<sup>13</sup> On the same day in La Ferté-Bernard, a recently released jihadi attempted to harm a taxi driver while recording a video claiming to act in the name of Islam; the victim escaped, and the attacker was arrested by police.<sup>14</sup> Although neither attack disrupted the Olympic events, they demonstrated the continued ability of extremist actors to commit violence and reinforced the need for heightened security during the Games.

To counter these risks, French authorities implemented an exceptionally heavy law enforcement presence in Paris and across the Île-de-France region, deploying approximately 35,000 police and gendarmerie officers daily over the 17 days of competition.<sup>15</sup> This large-scale mobilization not only served as a visible deterrent to potential attackers but also provided rapid response capabilities to contain and neutralize emerging threats. The effectiveness of this approach was demonstrated by the arrest of a 16-year-old jihadi from Haute-Savoie, who was reportedly planning an attack on the La Défense business district in the western suburbs of Paris. Intelligence suggested that he had targeted La Défense specifically because the intensive policing operation in central Paris would have reduced the likelihood of success there.<sup>16</sup>

### **Sabotage**

In the hours leading up to the opening ceremony of the 2024 Summer Olympics in Paris, France's high-speed rail network was the target of a coordinated series of arson and sabotage attacks that disrupted travel across the country and into the host city. In the early morning of July 26, 2024, saboteurs set fires and caused damage along multiple LGV high-speed lines that connect Paris with cities in the north, west, and east, throwing critical rail infrastructure into chaos just as international athletes, officials, and spectators were arriving for the Games.<sup>17</sup> French rail operator SNCF reported that three major lines—LGV Atlantique, LGV Nord, and LGV Est—suffered “malicious acts” that led to widespread delays and cancellations affecting hundreds of thousands of passengers, and another attempt on the LGV SudEst line was thwarted by rail workers who were on site.<sup>18</sup> Authorities described the incidents as “acts of sabotage” that were “prepared and coordinated,” and French intelligence services were mobilized to investigate.<sup>19</sup>

The timing and scale of the attacks immediately raised alarms among both French officials and international observers, given their spatial and temporal proximity to one of the most globally significant sporting events. Paris transport hubs such as Montparnasse and Gare du Nord experienced significant disruption, with delays rippling through national and international routes, including services operated by Eurostar, which reported the cancellation of approximately one-quarter of its trains due to the damage.<sup>20</sup> The scale of the disruption was significant with reports suggesting that up to 800,000 travelers were affected by delays and cancellations, with some international delegations forced to adjust travel plans on short notice.<sup>21</sup>

Despite extensive security operations in place for the Olympics, no group immediately claimed responsibility for the sabotage, and

authorities did not publicly attribute the acts to a particular terrorist organization or foreign state at the time.<sup>22</sup> Some domestic political figures, including France's interior minister, suggested that far-left extremists might have been involved, reflecting concerns over politically motivated sabotage by groups opposed to the Games or state authority.<sup>23</sup> However, these suggestions remained speculative, and official investigations were ongoing. Some international voices even advanced unverified claims of state-linked involvement, illustrating how such incidents can quickly become entangled in broader geopolitical narratives even without verifiable evidence.<sup>24</sup> What was clear from reporting was that the attacks exposed vulnerabilities in critical infrastructure at a moment of heightened national and international attention, underscoring the importance of protecting the supply chain to the major event as well as the need for comprehensive security planning that extends beyond stadiums and into the wider transportation networks upon which such events depend.

A few days later, another act of sabotage occurred. In this case, fiber optic cabling was destroyed in five locations, the impact of which was that telecommunications and internet services were affected in nine French departments,<sup>25</sup> although no link to the attacks on the rail infrastructure was established at the time and the perpetrators were never identified.

### **Cyber Incidents**

In line with trends observed during previous major international sporting events,<sup>26</sup> cybersecurity formed a key part of the threat environment during the 2024 Summer Olympics, with French authorities confronting a significant number of cyber incidents directed at organizations involved in the preparation and execution of the Games. Responsibility for monitoring and responding to cyber threats was led by *Agence nationale de la sécurité des systèmes d'information* (ANSSI), France's national cybersecurity agency, which coordinated protective security measures across government institutions, Olympic organizers, and private-sector partners.<sup>27</sup> Its cybersecurity approach to the Olympics focused on five main areas: understanding cyber threats; securing critical systems; protecting sensitive information; raising awareness among all stakeholders; and responding rapidly if incidents did occur. Nearly 500 organizations involved in the Games (ranging from venues to service providers) were risk assessed and received technical guidance, security audits, and support for their organizational resilience to cyber attacks.<sup>28</sup>

During the Games, 548 cybersecurity events were recorded, ranging from attempted intrusions to temporary system outages. Most cyber incidents were minor and required little or no intervention, while 83 were confirmed breaches.<sup>29</sup> About half of all reported cyber incidents during the Games involved service outages, including distributed denial-of-service attacks, with the remainder comprising attempted intrusions or exploitation of known or suspected system vulnerabilities. Crucially, none of these incidents disrupted competitions or key Olympic operations, demonstrating that the preventive measures, monitoring, and coordination put in place were effective. Although the cyber security measures successfully mitigated major disruptions, the rapid evolution of digital tools and increasingly sophisticated attack methods means that future events will face a far more complex cyber threat landscape.

### *Unmanned Aerial Systems*

Unmanned aerial systems (UAS, sometimes described as drones) are now a frequent threat to most major public events. UAS offer the capacity to reach venues, areas, and individuals that have been traditionally well protected through extensive protective security planning, and were a significant security concern during the 2024 Paris Olympics and the preceding three-week-long Olympic Torch relay. With the assistance of their Spanish and British counterparts, the French security services were able to conduct 350 missions led by the French Air Force,<sup>30</sup> which resulted in 90 interceptions of UAS and the arrest of 85 UAS pilots during the period of the Games.<sup>31</sup> The vast majority of these arrests were “mainly tourists unaware of the regulations,” but at least one case of UAS-use to deliver contraband into a jail was prevented during the Olympics through the use of anti-UAS operations in proximity to the Roissy Charles de Gaulle Airport.<sup>32</sup> Public authorities had launched targeted campaigns ahead of the Games, including Europe-level messaging on drone safety, to warn hobbyist pilots and visitors that flying near Olympic venues and critical infrastructure was prohibited and to emphasize the safety and legal consequences of violations.<sup>33</sup>

UAS offers those seeking to cause disruption and harm new tactics and methods of planning an attack that were previously unavailable. In 2024, the investigation into an attempt to assassinate then presidential candidate Donald Trump at a rally in Pennsylvania identified that the perpetrator flew a drone over the site of the rally in the lead-up to the event, with media speculating that the assailant used the UAS to conduct reconnaissance in the days leading up to the attack, although his motivations are still unknown.<sup>34</sup> Similar deployments have been seen internationally where threat actors have also used UAS in their attack planning.<sup>35</sup> Their ability to extend the distance and methodology of a threat actor, as well as enable physical protective security measures to be breached from the air, has caused significant concern for security planners in recent times<sup>36</sup> and will be a continuing concern for any future major events, including the 2026 World Cup. Their ease of access through affordable, commercial, off-the-shelf UAS has resulted in extensive use among organized crime gangs in Central and South America as well as terrorist and extremist groups in North America and Western Europe with France and Belgium identifying at least four recent incidents involving the use of drone by jihadis, including a plot to target Belgian Prime Minister Bart De Wever with a drone carrying an IED in 2025.<sup>37</sup> Unmanned aerial systems therefore pose a complex threat to major sporting events, offering bad actors a new capacity for disruption and physical harm.

### *General Crime*

Beyond directed actions against the events themselves, incidental threats such as general crime should also be a consideration for organizers. During the 2024 Paris Olympics, the heavy law enforcement presence led to a drop of criminal acts such as assault, theft especially in public transport, auto theft, vandalism, and fraud in the Parisian region but also, surprisingly, in the rest of the country.<sup>38</sup> Gendarmes and police officers arrested 736 people for general criminal acts related to the Olympics, including 451 in the Parisian region. According to the French Ministry of Justice, 212 of these arrests led to pursuits for fraud and economic crimes (41 percent), and for fights, traffic violations, and unlawful drone use (44 percent).<sup>39</sup>

The improvement in public safety as a result of the significant

deployment of security personnel was noticeable and commented upon by various national newspapers, leading to a public request for a continuation of “the Olympic truce.”<sup>40</sup> In Marseille, authorities announced they were looking at continuing the “legacy” of the Olympic security apparatus due to its efficiency;<sup>41</sup> however, the danger, similar to the Olympics in London in 2012 and the Commonwealth Games in Glasgow in 2014, is that the security operation and reduction in crime creates public expectations of safety and security that outlast the events themselves but that are difficult to sustain due to resource constraints.<sup>42</sup>

### **General Lessons from Paris**

Despite numerous concerns regarding its organization, the 2024 Paris Olympics took place from July 26 to August 11 without any major security incidents. The opening ceremony on the Seine River and the 17 days of competition that included 10,500 athletes and attracted close to 10 million spectators were secured by an important security apparatus in the Parisian region. The attacks in Israel in October 2023 and the Russia-Ukraine conflict added a much greater complexity to the threat environment for the Games. The 2026 World Cup will take place in 16 host-cities across three countries and over 39 days. Between five and seven million spectators are expected to attend the more than 100 games. The current conflict in Iran makes the competition, which is expected to be followed by several billions people across the world, an attractive target for those threat actors who find it purposeful to target civilians or embarrass the countries hosting the competitions. Another area of concern is the power of the cartels in Mexico, one of the host countries of the World Cup, which demonstrated their propensity to engage in violence, cause disruption, and instill fear after the killing of CJNG leader Nemesio Oseguera Cervantes (“El Mencho”) in February 2026.<sup>43</sup> This will surely be a consideration for organizers should there be a security incident or operation that impacts these organizations during the World Cup.

Lessons from the Paris Olympics are therefore useful in planning a safe and controlled 2026 World Cup. The Mexican, Canadian, and U.S. security apparatus will have to maintain close cooperation in a complex, diverse, and extremely vast sporting environment, despite differences in language and security culture. As G.B. Jones, FIFA’s chief safety and security officer for the 2026 World Cup, has observed, delivering “104 matches in 16 cities in three nations in 39 days” means there is “no handbook” for this tournament and no single domestic agency structure comparable to earlier World Cups.<sup>44</sup> The heavily centralized French security apparatus made internal cooperation between the Police Nationale, Gendarmerie Nationale, and their counterparts in the armed forces and intelligence services simpler than between the various federal, state, tribal, and local agencies of the three organizing countries. The threat environment will also be diverse, from potential riots and organized crime to possible terrorist events taking place in a polarized international context. Therefore, proactive security operations against potential threat actors should be implemented as early as possible.

The counterterrorism efforts in France in the spring leading up to the Olympics proved to be effective and had both short- and long-term effects. Due to the number of facilities and the different levels of readiness of the staff and law enforcement agencies, preparing and training are crucial. The risk for violence, rioting, or chaos will be greater from soccer fans than from the Olympics

attendees, particularly when events at past soccer tournaments are considered.<sup>45</sup> Procedure and responses have to be tested and drilled repeatedly before the beginning of the competition in order to ensure adequacy if an incident were to occur. Finally, security legacy has to be considered long before the end of the 2026 World Cup. The general public will be expecting some if not most of the effects of the security efforts to remain after the competition, leading to complaints about the security posture afterward. Some specific lessons for major sporting events, including the World Cup, follow below.

### **The Importance of Preventive Counterterrorism Measures**

A central lesson from Paris 2024 is the effectiveness of preventive, intelligence-led counterterrorism policing. French authorities disrupted multiple attack plots in advance of the Games and implemented legal controls on individuals assessed as posing a risk. These measures, combined with sustained monitoring of known extremists, probably reduced the likelihood of attack during the event itself. For the 2026 World Cup, it will be essential to ensure that such preventive approaches are effectively coordinated across jurisdictions. Given the transnational nature of the tournament and the current instability linked to conflicts in the Middle East, aligning threat assessments, developing mechanisms to share data and intelligence, and operational responses across host nations will be critical to mitigating risk.

### ***Securing Critical Infrastructure and Crowded Places as a Key Part of Event Security***

The coordinated sabotage of France's high-speed rail network immediately prior to the opening ceremony highlighted the vulnerability of infrastructure systems that underpin major events. Although the attacks did not directly target Olympic venues, they caused widespread disruption and demonstrated how adversaries can exploit vulnerabilities to generate impact. This reinforces the need for the World Cup and other major events planners to adopt a systems-based approach to security, extending beyond stadiums to include transportation, telecommunications, and energy networks, as well as the supply chain to these events.<sup>46</sup> Major events rely on complex interdependencies, and disruption to any one component can have cascading effects physically or reputationally. Indeed, Jones, in his recent interview in this publication, highlighted similar concerns with aviation capacity, warning that even routine weather delays at U.S. hub airports can rapidly cascade into large-scale displacement of travelers and accommodation pressures, a risk that will be amplified by the approximately five million people traveling to the United States alone for the World Cup.<sup>47</sup>

### ***Cybersecurity as a Core Security Pillar***

Cybersecurity was a prominent feature of the Paris threat environment and that of other major events.<sup>48</sup> Hundreds of cyber incidents were detected and managed, none of which disrupted core Olympic functions. This outcome underscores the effectiveness of a proactive approach centered on early risk identification, comprehensive stakeholder coordination, and the capacity for rapid, real-time response. Looking ahead to future major events, cybersecurity must be understood as a core operational domain rather than a supporting function. The increasing digitization of event infrastructure, including ticketing systems, communication platforms, and logistical networks, significantly expands the

potential attack surface available to threat actors. In parallel, the persistence of geopolitical instability is likely to sustain the risk of disinformation campaigns and politically motivated cyber activity.

### ***Addressing the Expanding Threat of Unmanned Aerial Systems***

The Paris Olympics demonstrated the growing relevance of UAS as a security concern. Numerous unauthorized drones were detected and intercepted, although the majority of these were tourists who were unaware of the regulations. Nevertheless, the accessibility and versatility of drone technology make it an attractive tool for a range of threat actors, from criminals to extremists. For major event security planners, counter-UAS capabilities will be essential moving forward and must be considered at the outset of planning—particularly when considering the unintentional disruption that counter-UAS technology can create when considered late in the planning phases. This includes not only technological solutions but also clear legal frameworks and public communication strategies. As recent studies have shown, drones are increasingly being incorporated into surveillance, disruption, and attack planning by both state and non-state actors.<sup>49</sup> They are also being used for planning for security at major events. As noted by Jones, drones and counter drone systems are among the newest emergent threats facing the tournament and FIFA has created a dedicated airspace security team to work with U.S., Canadian, and Mexican authorities on consistent mitigation and airspace domain awareness across the World Cup footprint.<sup>50</sup>

### ***The Importance of Deterrence***

The large-scale deployment of police and security personnel during Paris 2024 contributed not only to counterterrorism efforts but also to a broader reduction in general crime. However, deterrence in contemporary security environments extends beyond the visible presence of police and security personnel and increasingly depends on the active participation of private sector stakeholders as well as the public. Operators of venues, transport systems, crowded places, and digital infrastructure play a critical role in reinforcing security through the implementation of protective security measures as does the dissemination of clear, security-minded communications. Similarly, informed event attendees and citizens, encouraged through targeted awareness and deterrence messaging, can act as an additional layer of deterrence.

### ***Engaging Spectators and Tourists in Prevention***

Paris 2024 underscored that preventative security is not solely the responsibility of states and law enforcement agencies, but it also depends on the informed behavior of spectators, tourists, and other visitors. Public-facing guidance produced ahead of the Games was multi-tiered. Public officials provided practical crime prevention advice, which emphasized information about cyber hygiene and instructions on how to respond to suspicious activity, while private security providers and transport operators issued their own tailored messages for ticket holders and travelers.

There is significant value for future major events, including the 2026 FIFA World Cup, in developing a similarly integrated communication strategy that uses clear, accessible language. This should include consistent approaches on how to report concerns, simple and clear explanations of venue and transport security measures as well as digital-security advice for those using official web and mobile applications and online ticketing services. By

shaping visitor expectations and encouraging basic security-minded behaviors in advance, organizers can reduce inadvertent rule-breaking and create an additional layer of resilience around more traditional policing and protective security measures.

## Conclusion

The experience of the 2024 Summer Olympics demonstrates that major events can be secured effectively, even in a high-threat environment, when supported by integrated, adaptive, and

intelligence-led security arrangements. For major events, such as the 2026 FIFA World Cup, the central challenge will lie less in replicating the operational measures adopted in Paris and elsewhere and more in adapting and scaling them across a multi-jurisdictional context where differing legal systems, institutional arrangements, and threat environments exist. The five lessons identified should therefore be understood not as a formal framework, but as insights for strengthening future event security planning. **CTC**

## Citations

- 1 "FIFA World Cup 2026: Fixtures, groups, teams, tickets, host countries, cities and more," FIFA.com, March 29, 2026.
- 2 "500 days to go: excitement builds for FIFA World Cup 26," FIFA.com, January 27, 2025.
- 3 Ramón Spaaij, "Terrorism and Security at the Olympics: Empirical Trends and Evolving Research Agendas," *International Journal of the History of Sport* 33:4 (2016): pp. 451-468.
- 4 Alexandre Rodde, David McIlhatton, John Cuddihy, and Rachel Monaghan, "Protecting Major Sporting Events from Terrorism: Considerations for the Paris Olympics and Beyond," *CTC Sentinel* 17:6 (2024).
- 5 Alexandre Rodde, "Terrorism in France: Overview of the French Extremist Movements in 2024," National Gendarmerie Research Center, January 2025.
- 6 "La justice suspend une mesure de surveillance d'une adolescente de 17 ans, soupçonnée de constituer une menace pour la sécurité publique," *Parisien*, August 22, 2024.
- 7 "Corse : armés et cagoulés, trois militants du FLNC font irruption lors d'un rassemblement d'indépendantistes," TF1, August 5, 2024.
- 8 Ibid.
- 9 Vincent Le Goff, Clément Tronchon, and Sébastien Bonifay, "Le FLNC s'invite aux journées internationales de Corte," Franceinfo, April 8, 2024.
- 10 "Arrest of Mohammed Merah's brother-in-law, on S file and wanted, 100m from the Vincennes fan zone," *Entrevue*, August 10, 2024.
- 11 "Le beau-frère du terroriste islamiste Mohammed Merah, fiché S, interpellé à Vincennes," *Figaro*, August 11, 2024.
- 12 For information on fiche S, see "Terrorisme : qu'est-ce que la fiche 'S'?" *Monde*, October 16, 2023.
- 13 Alexandre Chassignon, "Agression de surveillants à la prison de Laon: fin de garde à vue pour Ali Riza Polat," *Parisien*, July 23, 2024.
- 14 Alexandre Chassignon, "Agression d'un chauffeur de taxi en Sarthe : le suspect envisageait d'attaquer la synagogue et un cinéma du Mans," *France Bleu*, August 9, 2024.
- 15 "Sécurité des JO 2024 : audition de M. Gérard Darmanin, ministre de l'intérieur et des outre-mer, sur la sécurité des jeux Olympiques et Paralympiques de 2024," Sénat, October 25, 2022.
- 16 Rodde, McIlhatton, Cuddihy, and Monaghan.
- 17 Lipika Pelham and Paul Kirby, "French high-speed rail sabotaged before Olympic ceremony," *BBC*, July 26, 2024.
- 18 Leila Abboud, Sarah White, Adrienne Klasa, Sara Germano, and Sam Jones, "The Paris Olympics sabotage attack: what we know so far," *Financial Times*, July 26, 2024.
- 19 "'Sabotage' hits French trains hours before Olympics," *France24*, July 26, 2024.
- 20 "Who was behind the arson attacks on railways before the Olympics?" *Foreign Affairs*, July 26, 2024.
- 21 Tara Cobham, "Saboteurs launch 'malicious' arson attack on France's rail networks hours before Paris Olympics," *Independent*, July 26, 2024.
- 22 Catherine Porter and Aurelien Breeden, "Rail Sabotage Blights an Olympic Moment for France," *New York Times*, July 26, 2024.
- 23 Daniel Boffey, "Far left behind rail sabotage before Olympics, French minister suggests," *Guardian*, July 29, 2024.
- 24 Adam Parsons, "Paris 2024: Who would cause such chaos on France's rail network before the Olympics, and avoid claiming publicity?" *Sky News*, July 27, 2024.
- 25 "Sabotage : des réseaux de fibre optique visés," *Franceinfo*, July 30, 2024.
- 26 Rodde, McIlhatton, Cuddihy, and Monaghan.
- 27 "Bilan cyber des Jeux Olympiques et Paralympiques de Paris 2024," Agence nationale de la sécurité des systèmes d'information (ANSSI), September 10, 2024.
- 28 Ibid.
- 29 Ibid.
- 30 "JOP 2024 : bilan de la sécurisation aérienne," Ministère des Armées, September 11, 2024.
- 31 "Comptes rendus de la commission des affaires étrangères, de la défense et des forces armées," Sénat, October 22, 2024.
- 32 "JOP 2024 : bilan de la sécurisation aérienne."
- 33 See "Drone Safety During the Paris Olympics," European Union Aviation Safety Agency, July 23, 2024.
- 34 "Trump gunman flew drone over rally site hours before shooting the former president," *Sky News*, July 20, 2024.
- 35 Nina Kurt, "Weaponised Skies: The Expansion of Terrorist Drone Use Across Africa," *GNET*, July 30, 2025.
- 36 Peter Suci, "Drone Threat Rising As The U.S. Will Play Host To High Profile Events," *Forbes*, November 14, 2025.
- 37 "En Belgique, un projet d'attentat djihadiste visant le premier ministre Bart De Wever a été déjoué, selon la police," *Monde*, October 9, 2025.
- 38 "Tableau de suivi statistique de la délinquance enregistrée pendant les JOP 2024," Ministère de l'Intérieur, September 19, 2024.
- 39 "Sécurité des Jeux olympiques de Paris 2024 : un bilan 'très très bas' de la délinquance," *Sud Ouest*, August 18, 2024.
- 40 Geoffroy Branger, "JO Paris 2024 : l'amélioration de la sécurité, constatée dans la capitale, pourrait-elle perdurer?" *Europe 1*, August 12, 2024.
- 41 Denis Trossero, "Bilan de la sécurité estivale à Marseille : une délinquance en baisse," *Mesinfos*, September 19, 2024.
- 42 Dina Rickman, "London 2012: Crime Dropped By 6% During Olympic And Paralympic Games, Bernard Hogan-Howe Says," *Huffington Post*, November 8, 2012.
- 43 Vanessa Buschschlüter and Otilie Mitchell, "Cartel henchmen unleash violence after top drug lord killed in Mexico," *BBC*, February 23, 2026.
- 44 Brian Dodwell and Don Rassler, "A View from the CT Foxhole: G.B. Jones, Chief Safety and Security Officer, FIFA World Cup 2026," *CTC Sentinel* 19:3 (2026).
- 45 Sam Cunningham, "I've witnessed Euros violence up close – England fans are at serious risk," *The Paper*, June 13, 2024; "South American Football Cup: Violence, Upsets, Surprising Twists," *Latin American Post*, April 18, 2025; Mario Cortegana and Dan Kilpatrick, "Violence in Mexico forces suspension of soccer games; Mexican Open to go ahead," *New York Times*, February 23, 2026.
- 46 Rodde, McIlhatton, Cuddihy, and Monaghan.
- 47 Dodwell and Rassler.
- 48 Samiksha Jain, "Russian Cyberattacks Target Milan-Cortina Winter Olympics Ahead of Opening Ceremony," *Cyber Express*, February 5, 2026.
- 49 Mohammad Eslami and Lauro Borges, "Drones Beyond the State: Non-state Actors and the Evolving Threat Landscape" in *The Drones Race and International Security, Contributions to Security and Defence Studies* (Cham, Switzerland: Springer, 2025).
- 50 Dodwell and Rassler.