Department of Political Science *Course of Security Policies*

Comparative Analysis of Security Challenges and Policy Responses in the 2012 London and 2024 Paris Summer Olympics

SUPERVISOR: *Prof. Carlo Magrassi* **CANDIDATE:** *Hugo HERAUD*

CO-SUPERVISOR: *Prof. Paolo Ciocca* **CANDIDATE ID:** *655782*

ACADEMIC YEAR 2024/2025

Abstract:

The Olympic Games are known as global events that promote peace and cooperation. With this in mind, they are now increasingly focused on security operations. Therefore, this thesis explores how the way threats are framed affects Olympic security management and democratic accountability, specifically looking at London 2012 and Paris 2024.

Using securitization theory and discussions around exceptionalism, the study reveals that different views of threats led to different governance approaches. In London, the memory of the 2005 bombings framed terrorism as a major risk. The failure of the private contractor G4S threatened its legitimacy, but parliamentary oversight, public accountability, and the visible strength of state institutions turned this crisis into evidence of resilience. In contrast, Paris 2024 faced a mix of security challenges, terrorism, cyber threats, and civil unrest, viewed as needing technological solutions. Algorithmic video surveillance, approved under Law n° 2023-380, helped keep the Games safe but raised important issues about fairness, openness, and the acceptance of exceptional measures.

This comparison shows that we cannot measure effectiveness solely by the lack of violence. Security management must also build trust and legitimacy. Without transparency, sunset clauses, and public involvement, Olympic security could turn into a way to permanently increase extraordinary powers.

Keywords: *Olympic Games, London 2012, Paris 2024, security governance, threat framing, policy reforms, democratic accountability, surveillance.*

Acknowledgments:

I would like first and foremost to express my sincere gratitude to my advisor Professor Carlo Magrassi who inspired me with his enthusiasm, unwavering optimism, and profound knowledge of security, as well as the wisdom of his life experience.

I would also like to thank Professor Paolo Ciocca as well as Dott. Federico Deiana for their valuable insights, timely feedback, and steady encouragement throughout this project. They were unfailingly available, no matter the hour or the question, and their guidance sharpened my arguments, strengthened my methods, and kept the work moving forward.

Finally, I owe my deepest gratitude to my parents, who instilled in me the values that guide my life, supported me financially throughout my studies, and encouraged me at every stage of researching and writing this dissertation.

Table of contents:

Introduction:

Since their modern revival in Athens in 1896, the Olympic Games have been more than an athletic competition. They have been stages on which nations projected identity, prestige, ideology and power under the site of the world. From Berlin 1936, where the Games were used as a propaganda tool by the nazi regime, to Mexico City 1968, where American athletes Tommy Smith and John Carlos raised their fists in the Black Power salute, they turned the Olympic podium into a powerful act of defiance, forcing the world to confront the violence and discrimination that African Americans endured back home.[1] The elements have shown us how the Olympics have always mirrored the political and social tensions of their time and age. Each edition reveals not only the spirit of sport, but also the anxieties, ambitions, and values of the host society.

However, one element has become more and more important in the preparation and organization of this mega sport events: “the need for security". If the Cold War era showcased ideological rivalries between the eastern and western blocks, the post-9/11 era has turned the Olympics into high-stakes security operations, rivalled only by summits such as the G20 and G7 (previously the G8). Stadiums and fan zones carry the symbols of peace and cooperation, despite the fact that they are encircled by checkpoints, soldiers, and, more recently, AVS (Algorithmic Video Surveillance). The Games are therefore not only sporting events but also fortresses, laboratories, and mirrors all at once. They are fortresses because they attract threats ranging from terrorism to cyberattacks. They are laboratories because they allow governments to test new powers and technologies under extraordinary conditions, thus justifying the use of new technologies for the years to come. And they are mirrors because the way security is framed and managed reflects what societies fear most and what they are willing to sacrifice in the name of safety.

Security at the Olympics is never just about neutralizing and anticipating risks. It is more a political act, shaped by narratives about danger and the exceptional measures they are said to require. A missile battery on a London rooftop in 2012, or an algorithm scanning Parisian crowds

[1] The Olympic Museum, *The Modern Olympic Games* (Lausanne: International Olympic Committee – The Olympic Museum, 2013).

in 2024, are not only protective choices; they are statements about how the government function and the type of governance they inflict on the population. They embody what is considered threatening, what is deemed acceptable, and how far democracy may bend under pressure. These narratives, also known as “threat framing”, matter profoundly. By doing so, they legitimize extraordinary laws, justify immense expenditures, and shape whether citizens experience security as reassurance or as intrusion.

This thesis examines how threat framing shapes Olympic security governance and democratic accountability, through the use of two important and pivotal case studies from the 21st of century: the London 2012 and Paris 2024 Summer Olympics and Paralympic Games.

London’s Games were haunted by the memory of the 2005 bombings, with terrorism framed as an existential threat demanding visible preparedness and institutional resilience.[2] The failure of the private contractor G4S to provide enough guards could have undermined public trust, yet parliamentary scrutiny, media debate, and military intervention reframed the debacle as proof of adaptability. As a result, the city of London demonstrated how a framing centered around terrorism, despite the implementation of significant exceptional measures, also compelled visible accountability.

Paris 2024 faced a different constellation of risks. France’s recent wave of terrorist attacks, between 2015 and 2016, combined with fears of cyberattacks, disinformation, and social unrest produced a more diffuse, hybrid threat framing. This justified experimentation with algorithmic video surveillance, authorized under Law n° 2023-380 as a temporary measure.[3] While the Games passed without major incident, critics such as La Quadrature du Net, Amnesty International France and Mediapart warned that temporary exceptions could quietly become permanent without anyone noticing. Paris thus succeeded technically but faltered politically: technological innovation did not automatically translate into democratic legitimacy.

Taken together, these two Games have illuminated and showcased central tensions within Olympic security. Effectiveness cannot be judged only by the absence of violence; it must also be measured by the presence of trust. Systems that protect but alienate may achieve short-term safety while undermining long-term legitimacy from the population. London revealed how

[2] Paul Birkett, “London 2012: Protecting the Olympic Games”*, Domestic Preparedness*, July 25, 2012.
[3] République française. “Loi n° 2023-380 relative à l’organisation des Jeux Olympiques et Paralympiques de 2024”. *Paris : Journal officiel de la République française*, 20 mai 2023.

openness and accountability could sustain trust, even amid failure. Paris showed that innovation without transparency risks leaving behind suspicion rather than reassurance.

The broader significance of this dynamic is clear. As past Olympics have shown, the Games are sites of securitization, where risks are magnified into existential threats demanding extraordinary responses. They are laboratories of security innovation, where exceptional measures often outlast the event itself. And they are theatres of perception, where security is judged not only by how it works but by how it feels, meaning whether the soldiers present on the streets are reassuring or intimidating the public, whether drones and algorithms are trusted guardians or symbols of intrusion. Each host city thus becomes a stage on which societies rehearse the fragile balance between freedom and control, spectacle and restraint.

Therefore, this thesis will be guided by my research question that is: How does threat framing shape Olympic security governance and democratic accountability in the cases of the London 2012 and Paris 2024 Summer Olympics and Paralympics? To answer this, the research situates Olympic security within broader debates on securitization, exceptionalism, and democratic governance. It shows how distinct threat framing, terrorism in London, hybrid risks in Paris, produced divergent security models and different consequences for accountability and legitimacy.

To answer this question, my thesis is structured into four parts. The first is a literature review that surveys existing academic work on the security governance and democratic accountability of London 2012 and Paris 2024. The second situates Olympic security in a broader context, tracing the history of securitization around mega-events and examining how threat framing shapes state responses. The third offers a comparative analysis of how the United Kingdom and France framed and constructed security threats in the lead-up to London 2012 and Paris 2024, showing how political culture, institutional memory, and strategic doctrine influenced their approaches and justified exceptional measures. The fourth and final part draws lessons and their future implications from these two cases, highlighting how Olympic security strategies affect future planning, democratic accountability, technological legacies, and public trust.

The Olympics are intended to celebrate peace, dignity, and cooperation. Yet the way they are secured reveals much about how democracies confront risk under pressure. Whether future hosts treat Olympic security as a shield against threats or as an opportunity to model

accountable governance will determine not only the legacy of their Games but also the credibility of democratic values in an age where security and freedom so often collide.

Part I – Literature review

Throughout my literature review, I will lay down the groundwork for my thesis by introducing the key debates around Olympic security. First, I will examine how mega-events are framed as sites of exceptional risk. Secondly, I am going to explain how surveillance technologies are assessed and normalized. Thirdly, I will take a look at how legal and institutional safeguards seek to limit extraordinary powers. In my fourth and final part, I will analyze how publics and media shape the legitimacy of these measures. Together, these perspectives show not only how the Games are secured, but also how those security choices reshape governance and democracy long after the closing ceremony.

A. Governing Mega-Events: Securitisation, Risk, and Exception

The governance of Olympic security must be situated within broader theoretical frameworks that explain how mega-events serve as catalysts for the expansion of state power and the normalization of exceptional security practices. Large-scale sporting events, also known as MSEs (Mega Sporting Events), such as the Summer Olympic and Paralympic Games not only draw massive crowds and global attention but also provide fertile terrain for the reconfiguration of public order and security governance. Concepts such as securitisation[4], states of exception[5], and risk governance[6] have provided critical lenses facilitating the examination of these never-ending transformations.

Securitisation: From Spectacle to Security Priority

[4] Barry Buzan, Jaap de Wilde, Ole Wæver, *Security: A New Framework for Analysis* (Boulder, CO: Lynne Rienner, 1998).
[5] Giorgio Agamben, *State of Exception*, trans. Kevin Attell (Chicago: University of Chicago Press, 2005).
[6] Claudia Aradau and Rens van Munster, "Governing Terrorism Through Risk: Taking Precautions, (Un)Knowing the Future," *European Journal of International Relations* 13, no. 1 (2007): 90.

The Olympic Games are often described as celebrations of peaceful international competition, unity, and human achievement. Despite this wanted and essential goal, beneath the surface of this spectacle lies an increasingly dominant concern, this one being the need for security. Over the past two decades, host cities have installed up efforts to protect the Games from a wide range of perceived threats, from terrorism and cyberattacks to civil unrest and political protest. This shift is not a coincidence; it is rather rooted in a broader process that scholars and academics have called securitisation.

Many have argued that securitisation occurs when political and security actors frame a particular issue as an existential threat, this is something that demands urgent and exceptional responses beyond the scope of normal democratic procedures.[7] As soon as a topic is successfully securitised, it is effectively moved outside the realm of regular politics and into a zone of emergency management. In this way, the mere possibility of danger, real or fictional, can justify extraordinary powers and justify long-term legal and institutional shifts.

Mega-events like the Olympics have offered and still to this day propose fertile ground for this kind of framing. Many have argued that these events act as "security amplifiers," meaning that they facilitate the capacity of a state to justify measures that might otherwise provoke resistance. The scale, symbolism, and international attention of the Games make them easy to portray as highly vulnerable targets.[8] National security actors often use the event to dramatize risks and position themselves as the guardians of safety, even in the absence of a concrete or imminent threat.

This dynamic was especially visible in the lead-up to London 2012. The memory of the 2005 7/7 London bombings, just a day after London won the Olympic bid, was extremely present in public discourse. Officials saw terrorism as a primary risk and framed the Games as a potential hot spot for attacks, thus the need to apply measures in alignment with this kind of threat.[9] [10] As a result, framing helped legitimise a vast expansion of security infrastructure and capabilities, including the deployment of 18,000 security personnel, anti-aircraft missiles on residential buildings, as

[7] Buzan, de Wilde, Wæver, Security.
[8] Philip Boyle, Kevin D. Haggerty, "Planning for the Worst: Risk, Uncertainty and the Olympic Games," *British Journal of Sociology* 63, no. 2 (2012): 241–59.
[9] United Kingdom. Home Office. *London 2012 Olympic and Paralympic Safety and Security Strategy*. March 2011. Published by the Home Office.
[10] Joep van de Weijer, *Securitization and the London 2012 Olympic Games: A Discourse Analysis* (Wageningen: Wageningen University, 2016).

well as extensive public surveillance networks.[11] [12] Security was no longer just a logistical concern; it became a fundamental issue to how the Games were governed and understood.

Something similar appeared before the start of Paris 2024, despite being in a more technologically advanced context. French security agencies, including the SGDSN (Secrétariat Général de la Défense et de la Sécurité Nationale) and military-affiliated think tanks, have emphasised the threat of terrorism, cyber warfare, and hybrid attacks. This framing has supported the introduction of controversial technologies like algorithmic video surveillance, authorised under Law No. 2023-380.[13] These AI tools, which introduced the possibility of scanning behavioural anomalies such as crowd congestion or abandoned luggage, are publicly justified as necessary to prevent catastrophic incidents, despite significant legal and ethical concerns, that have been often criticized by non-profit organisations, academics and medias.[14] [15]

What securitisation does in both cases is reframe everyday logistical or organisational problems, like how to manage large crowds or ensure safe transport, not merely as technical challenges, but as potential security threats. Once this shift in discourse occurs, authorities are empowered to act in ways that exceed ordinary democratic norms, often with little resistance. Academics such as Coaffee[16] and Fussey[17] have pointed out that securitisation of mega-events opens up legal and operational grey zones where the normal rules can be bent, changed or suspended. Surveillance becomes not just a precaution but a necessity. Military deployments are now not extraordinary, but something that is expected.

Crucially, securitisation is not just a rhetorical exercise, it enables real policies, real deployments, and real changes to the governance of public space. The Olympic city becomes not only a host to athletes and fans, but also a site of managed suspicion and heightened surveillance. This

[11] Pete Fussey, "Command, Control and Contestation: Negotiating Security at the London 2012 Olympics," *The Geographical Journal 181*, no. 3 (September 2015): 212-223.
[12] Nick Hopkins, Owen Gibson, and Hélène Mulholland, "G4S Faces Financial Penalties over Olympic Security Failures," *The Guardian*, July 12, 2012.
[13] République française, *Loi n° 2023-380*, 20 mai 2023.
[14] Luba Zatsepina and Jan Andre Lee Ludvigsen, "Algorithmic Olympics : Exploring the Ethical and Social Implications of AI Surveillance through the Case of Paris 2024," *Surveillance Studies Journal* (2024).
[15] Amnesty International France, "JO 2024 : Pourquoi la vidéosurveillance algorithmique pose problème," April 15, 2024.
[16] Jon Coaffee, "Evolving Security Motifs, Olympic Spectacle and Urban Planning Legacy: From Militarization to Security-by-Design," *Planning Perspectives* 39, no. 3 (2024): 637–57.
[17] Fussey, "Command, Control and Contestation".

transformation has long-term implications, as the tools and logics developed under the banner of Olympic security often persist well beyond the event itself, subtly reshaping the relationship between the state and its citizens.

States of Exception: Law, Suspension, and Normalisation

If securitisation explains how issues are framed as urgent threats, Giorgio Agamben's concept of the state of exception[18] helps us understand what happens next. In a state of exception, normal legal rules are suspended under the justification of the emergency we live in. This suspension allows the state to act in ways that would otherwise be considered unlawful or illegal, such as restricting movement, extending surveillance, or curtailing civil liberties. It is important and even essential to not that while these measures are presented as temporary, history has shown us that they often leave lasting marks, becoming quietly integrated into the routine operations of governance.

Mega sporting events such as the Olympics are perfect examples of where this logic comes from. Their scale and symbolism provide governments with strong political justification to push through exceptional legal frameworks, usually in the name of protecting the Games from catastrophic harm. But as scholars note, once in place, these extraordinary measures tend to outlive the event itself.[19] [20]

This was visible during London 2012, where the United Kingdom's 2008 Counter-Terrorism Act as well as few Olympic-specific laws facilitated measures such as pre-emptive policing, expansive stop-and-search powers, and widespread surveillance.[21] [22] These measures were justified as necessary to prevent another "7/7-style" attack, but their scope went well beyond

[18] Agamben, *State of Exception.*
[19] Coaffee, *Evolving Security Motifs*.
[20] Boyle and Haggerty, *Planning for the Worst*.
[21] United Kingdom, *London 2012 Olympic and Paralympic Safety and Security Strategy*, March 2011.
[22] House of Commons Committee of Public Accounts, *The London 2012 Olympic Games and Paralympic Games: post-Games review*, Fortieth Report of Session 2012–13 (HC 812), London: The Stationery Office, published 19 April 2013, ordered printed 18 March 2013.

the Games themselves. Critics argued that the event accelerated the instalment of counterterrorism practices into everyday policing and urban governance.[23]

During Paris 2024, this dynamic resurfaced in an even sharper form. The adoption of Law No. 2023-380 authorised, for the first time in France, the experimental deployment of algorithmic video surveillance in public spaces.[24] While the law explicitly prohibited facial recognition, it allowed AI systems to monitor behaviours such as crowd anomalies, loitering, or sudden movements. Importantly, the law extended this experiment until March 2025, after the Games were scheduled to end. Civil liberties organisations such as La Quadrature du Net[25] and Amnesty International France[26] denounced this as a dangerous precedent, warning that temporary experimentation could become a gateway to permanent surveillance infrastructures.

What emerges here is a familiar pattern: the organisation of the exceptional under the umbrella of necessity or experimentation. By embedding extraordinary powers into law, governments normalise practices that were initially justified as temporary. Academics such as Aradau and Van Munster warn that such measures are often justified not by concrete threats but by possible futures.[27] The risk of an attack, or even the uncertainty of what might happen, becomes enough to suspend normal rules. In this way, the exceptional does not end with the Games, it risks becoming the new norm.

Risk Governance: Managing the Unknown

If securitisation frames the Olympics as sites of existential threat, and the state of exception explains how laws are bent to address them, risk governance helps clarify the everyday logic that maintains these extraordinary measures. Ulrich Beck's influential idea of the risk society describes a world where governance is more about anticipating potential dangers

[23] Fussey, *Command, Control and Contestation*.
[24] République française, *Loi n° 2023-380*, 20 mai 2023.
[25] La Quadrature du Net. *Algorithmic Video Surveillance, Dangers and Counter-attacks*. Paris : La Quadrature du Net, 2023.
[26] Amnesty International France, *JO 2024 : Pourquoi la vidéosurveillance algorithmique pose problème*.
[27] Aradau and van Munster, *Governing Terrorism Through Risk*.

rather than responding to the concrete ones.[28] Threats present in our current societies are more often diffuse, invisible, and transnational, terrorist networks without borders, cyberattacks launched anonymously, or pandemics that spread globally. In such an environment, security shifts from reacting to known dangers to preparing for unknown possibilities.

This way of thinking became highly visible during the preparations for London 2012. The Olympic Safety and Security Strategic Risk Assessment (OSSSRA) classified risks not only by type but by their likelihood and impact, providing a template for decision-making.[29] As a result, this framework did not wait for threats to materialise. Instead, it sought to identify and mitigate vulnerabilities in advance, emphasising resilience-building, the capacity to withstand shocks, and interoperability, or the seamless coordination of multiple agencies. As Jennings and Lodge have shown, risks were rendered governable through classification, simulation, and anticipation.[30] In other words, potential crises were turned into adaptable scenarios, rehearsed and planned for even if they never came to pass.

By the time of Paris 2024, this logic had evolved into something even more tightly bound to data analytics and algorithmic prediction. Rather than relying solely on human assessments, French authorities leaned heavily on technologies designed to distinguish "normal" from "anomalous" behaviour in real time. AI-powered systems, such as CityVision developed by Wintics, were deployed across metro stations and Olympic venues to flag unattended bags, unusual crowd flows, or individuals moving erratically.[31] [32] These technologies embody what Aradau and Van Munster call a "pre-emptive security rationality" meaning a form of governance that acts not on actual events but on statistical possibilities.[33] The future becomes a space where risk must be managed, and machines and artificial intelligence are tasked with making that future legible and understandable.

---

[28] Oleg Komlik, "Ulrich Beck Has Died. His Powerful Concept of 'Risk Society' Is Relevant as Never Before," *Economic Sociology & Political Economy*, January 4, 2015.
[29] United Kingdom, *London 2012 Olympic and Paralympic Safety and Security Strategy*, March 2011.
[30] Will Jennings and Martin Lodge, *Tools of Security Risk Management for the London 2012 Olympic Games and the FIFA 2006 World Cup in Germany*, Discussion Paper No. 55 (London: ESRC Centre for Analysis of Risk and Regulation, November 2009).
[31] Chris O'Brien, Paris 2024 : *French Government Approves Controversial AI Video Surveillance*, *Forbes*, March 31, 2023.
[32] Wintics, *Cityvision : Détection d'anomalies pour les Jeux de Paris* (Paris : Wintics, 2024),
[33] Aradau and van Munster, "Governing Terrorism Through Risk".

While promising efficiency and speed, this approach carries profound implications. The reliance on algorithms risks humanizing security decisions, making them appear neutral or technical when they are in fact deeply political.[34] What counts as "anomalous" behaviour, for instance, is not an objective truth but a decision embedded in code, decided by programmers, policymakers, and security agencies. Coaffee warned us that such technocratic approaches privilege what can be quantified and predicted, often at the expense of less tangible concerns such as civil liberties, public trust, or social cohesion.[35]

As a result, risk governance at the Olympics highlights a paradox. On the one hand, it reflects a pragmatic effort to prepare for the worst in an uncertain world. On the other hand, by reducing complex human realities to calculable probabilities, it risks narrowing the very meaning of security. Instead of fostering public confidence, these systems may create a hidden layer of discretionary power, one that is harder to scrutinise precisely because it is masked as neutral technology.

Mega-Events as Laboratories of Security Innovation

Beyond their role as sporting spectacles, mega-events like the Olympics serve as laboratories for security innovation. Their unique characteristics, such as the fact that they last only for two weeks, thus a small duration, concentrated geography, and global visibility, these elements implement ideal conditions for testing measures that might be politically difficult to justify under normal circumstances. As Fussey observes, Olympic Games often act as *"testbeds of securitisation"*, meaning moments where new technologies and strategies first enter public life.[36] In these moments, the city becomes not just a venue for sport, but a controlled environment in which counterterrorism, policing, and surveillance methods can be deployed, observed, and refined, thus marking a new chapter in the security of the host nation.

[34] Fussey, *Command, Control and Contestation*.
[35] Coaffee, *Evolving Security Motifs*.
[36] Fussey, *Command, Control and Contestation*.

This experimental logic has been evident across different host cities. For example, London 2012 relied heavily on new inter-agency coordination protocols and large-scale crowd monitoring systems, developed partly in response to the memory of the 7/7 bombings. These practices did not vanish when the Games ended. Instead, they were absorbed into the broader policing and counterterrorism architecture of the UK, influencing everyday strategies of urban security.[37] [38] The Games provided a stage on which authorities could demonstrate their capacity to protect the nation, and, maybe most importantly, that the infrastructures they built endured long after the athletes had left, thus used professional athletes and everyday citizens alike.

Something similar took place during Paris 2024, though with a sharper focus on technological innovation. The adoption of algorithmic video surveillance under Law No. 2023-380 was framed as an Olympic experiment, designed to protect crowds in transport hubs, fan zones, and competition venues. Yet its authorisation extended until March 2025, and political debates have already surfaced about whether such systems should become permanent features of French urban life.[39] [40] The Olympics, in this sense, create opportunities to trial extraordinary technologies under the banner of necessity, with their normalisation often following in the years after.

This dynamic has raised pressing questions for democratic oversight. Scholars such as Boyle and Haggerty[41] as well as Aradau and Van Munster[42] have warned that mega-events risk becoming vehicles for redefining the limits of the possible in security governance. What begins as an exception to safeguard a festival of sport can quickly blur into everyday policing practice. Over time, the distinction between "temporary" and "permanent" erodes, as the exceptional logic of the Games folds seamlessly into routine governance. The Olympic city thus becomes more than a host; it becomes a proving ground for the future of surveillance and security.

[37] Fussey, *Command, Control and Contestation*.
[38] Committee of Public Accounts, *Post-Games review (HC 812)*.
[39] Léa Marie de Vergès, "Vidéosurveillance : attention à la dérive post-Jeux olympiques et paralympiques," *Le Monde*, September 26, 2024.
[40] Peter Caddle. "Paris Olympics' AI Mass-Surveillance System 'to Be Made Permanent,' Media Reports." *Brussels Signal*, October 2, 2024.
[41] Boyle and Haggerty, *Planning for the Worst*.
[42] Aradau and van Munster, *Governing Terrorism Through Risk*.

B. Surveillance Technologies and Urban Experimentation

Mega-events have for a long time accelerated the improvement and installation of surveillance tools, but the story is not merely one of more cameras or thicker perimeters, it is a story of datafication and the urban experiment. Early Olympic cycles foregrounded fixed CCTV networks, access control, and accreditation systems; Games that came after layered on biometrics, networked databases, and sensor fusion; and finally, Paris 2024, the most recent Olympics, fixed algorithmic video analytics, predictive models, and API-driven integrations with "smart city" infrastructures. Throughout my research of various surveillance theories, this arc reflects shifts in visibility and administrative watching mass data capture and correlation[43], the political ordering of everyday life through technical systems[44], and an encroaching surveillance capitalism that monetizes behavioural surplus.[45] For Paris 2024, these trends merged in the algorithmic turn, something that has been dubbed as the "Algorithmic Olympics" by Zatsepina and Ludvigsen.[46]

From seeing to sensing: the long arc of Olympic surveillance

The story of Olympic surveillance begins with CCTV, one of the most emblematic tools of late and early 20th century urban monitoring. In its earliest form, CCTV offered a primarily retrospective and human-mediated gaze: meaning a place where operators watched live feeds or replayed footage after an incident, relying on human attention to spot suspicious behaviours. This was limited and imperfect, however as Monahan pointed out, even the spread of such "low-tech" tools was never neutral.[47] It represented an early step in the reorganization of urban space around visibility and accountability, gradually normalising the expectation of being watched.

---

[43] Mark Andrejevic, "Big Data Surveillance: Introduction," *Surveillance & Society* 12, no. 2 (2014): 185–96.
[44] Torin Monahan, *Surveillance and Security: Technological Politics and Power in Everyday Life* (New York: Routledge, 2006).
[45] Shoshana Zuboff, "Surveillance Capitalism and the Challenge of Collective Action," 2019.
[46] Zatsepina and Ludvigsen, "Algorithmic Olympics".
[47] Monahan, *Surveillance and Security.*

By the late 2000s, however, the Olympic security handbook expanded far beyond cameras. Hosts cities began to experiment with biometric identification systems, Radio Frequency Identification (RFID) passes, and federated watchlists. These systems shifted surveillance away from simple watching to managing identities at scale, a transformation crucial for securing perimeters, controlling access to Olympic villages, and regulating the vast workforce. The transition from vision to data reflected a deeper political project: as Monahan argues, technologies of security do not just observe society; they profoundly redefine what counts as order and disorder by shaping how people move, gather, and interact.[48]

The 2004 Athens and 2008 Beijing Summer Olympic and Paralympic Games brought this shift into sharp relief. For example, in Athens, the city itself was reorganised as an instrument of control, covered with camera grids feeding into centralised command rooms.[49] On the other hand, Beijing went even further with this, as they weaved together dense surveillance infrastructures with multi-agency feeds, effectively fusing the Olympic city into a single, governable space.[50] These Games underscored how mega-events can offer governments a chance to conduct ambitious security architectures that would be politically controversial under ordinary conditions.

London 2012 marked the consolidation of this model. The integration of crowd-monitoring software, accreditation databases, and transport telemetry created a holistic security assemblage that operated in real time. Fussey highlighted how this assemblage extended well beyond the Olympic fortnight: the infrastructures and protocols pioneered during the Games seeped into routine policing and counterterrorism practice across the UK.[51] What was introduced as temporary became institutionalised as normal.

Across these cases, the Olympic city emerges as a laboratory of surveillance, bounded in time, symbolically charged, and politically permissive. In this environment, governments and private contractors can test tools that would otherwise face public resistance, from mass biometric scanning to algorithmic crowd analytics. The Games thus act not only as a showcase of athletic

[48] Monahan, *Surveillance and Security.*
[49] Minas Samatas, "Security and Surveillance in the Athens 2004 Olympics: Some Lessons from a Troubled Story," *International Criminal Justice Review* 17, no. 3 (September 2007): 220–238.
[50] Minas Samatas, "Surveillance in Athens 2004 and Beijing 2008: A Comparison of the Olympic Surveillance Modalities and Legacies in Two Different Olympic Host Regimes," *Urban Studies* 48, no. 15 (November 2011): 3347–3366.
[51] Fussey, *Command, Control and Contestation*.

excellence but also as a proving ground for new security technologies and governance models. What is tested in the "exceptional" space of the Olympics often migrates into the fabric of everyday urban life.

Datafication and the smart-event city

The move from simply watching to actively sensing represents more than a technical upgrade, it indicates a profound shift in how cities are governed during mega-events. Traditional CCTV produced images; operators then interpreted them, often quite lately. By contrast, contemporary surveillance infrastructures convert movement, identity, and presence into streams of data that can be cross-referenced, sorted, and acted upon in real time.

As Andrejevic pointed out, the promise of big data surveillance is not its sheer volume but the relations it constructs.[52] Pedestrian flows through ticket gates, RFID badge scans, mobile phone pings, and video frames are no longer discrete elements. Once networked, they form interoperable data ecosystems, capable of producing correlations and, more importantly, predictions about people and places. In this way, the Olympic city is transformed into an instrumented environment, where decisions increasingly derive from dashboards, anomaly alerts, and predictive heat maps rather than human intuition or observation.

This datafication carries a double edge. On the one hand, it offers efficiency as crowd surges can be detected early, abandoned objects identified instantly, and transport hold-ups managed dynamically. On the other hand, it also shifts the site of control. Zuboff reminds us that infrastructures built to predict and modify behaviour are never neutral.[53] The same systems that smooth pedestrian flows can be redeployed for behavioural governance, shaping how people move, where they gather, and what forms of presence are considered acceptable. Even more troublingly, once built, these data pipelines rarely remain confined to their original purpose. The flows of information generated for public safety may be repurposed, commercially, administratively, or politically, in ways far removed from their Olympic rationale.

[52] Andrejevic, *Big Data Surveillance*.
[53] Zuboff, *Surveillance Capitalism*.

In effect, the smart-event city is both a safety net and a sorting machine. It promises security and efficiency but also risks reducing public life to a series of data points, ranked and acted upon according to their predictive value. The challenge, then, is not only technical but political: how to balance the temptation of predictive efficiency with safeguards for rights, transparency, and the unpredictable richness of urban life.

The algorithmic turn: prediction as governance

The latest stage in Olympic surveillance has been marked with what might be called as the algorithmic turn, meaning the use of AI-powered systems that no longer simply record events but actively interpret them. As Zatsepina and Ludvigsen have observed, algorithmic video analytics change the very threshold of intervention.[54] Instead of relying on human operators to notice something unusual, machine-learning models are trained to categorise behaviour in real time, distinguishing between what is considered "normal" and what is flagged as "anormal."

This move represents a subtle but significant shift in the logic of security. Rather than asking "who" someone is, meaning the human focus on identity, it now asks "what they are doing". The result is a kind of post-biometric promise: policymakers have claimed that there is no facial recognition, and therefore no direct identification of individuals, while in reality surveillance is becoming more fine-grained than ever. Movement signatures, micro-gestures, or deviations from predicted paths can all become markers and elements of suspicion for authorities and security firms. The body itself is read as a dataset, constantly compared against algorithmic baselines of expected behaviour.

Authors such as Monahan argued that technical infrastructures reconfigure power "by material means" meaning something that is now quite literally embodied in code.[55] The training data used to teach models, the thresholds at which anomalies trigger alerts, and the classifications of risk embedded in the software all shape how police and stewards interpret public space.

[54] Zatsepina and Ludvigsen, *Algorithmic Olympics*.
[55] Monahan, *Surveillance and Security.*

Crucially, these parameters are rarely transparent. They quietly direct attention toward certain bodies, behaviours, or places, deciding in advance who or what counts as risky.

This opacity is one of the defining features that surrounds algorithmic governance. As Andrejevic notes, big data analytics operate on a logic of correlation rather than explanation.[56] An "anomaly" flag does not need to explain *why* a pattern is suspicious; it simply states that it deviates statistically from the norm. To those operating the system, this can appear as an authoritative signal. But to the public, and even to public institutions such as the government, it is often the case, because the inner workings of the model are inaccessible. In this way, algorithmic surveillance introduces not just a new technical tool but a new political reality: one in which authority rests less on human judgment and more on the enigmatic and puzzling outputs of artificial intelligence.

The algorithmic turn thus reframes governance itself. Prediction becomes policy; statistical deviation becomes grounds for intervention. While this promises speed and efficiency, it also risks normalising a world where opacity and automation displace transparency and accountability.

Urban experimentation and democratic friction

As Fussey[57] and Samatas[58] have argued, the Olympic host city is uniquely suited to serve as a testbed for security innovation. A mega-event such as the Olympics concentrates resources, compresses timelines, and benefits from a built-in presumption of necessity: the Games *must* go on, and they *must* be safe. Both of these elements are essential for the wellbeing of this event. This sense of urgency creates political room to experiment with tools and techniques that might otherwise face resistance.

But experiments rarely end when the closing ceremony fireworks fade. They leave legacies. The datasets collected during the Games often remain stored; the vendor ecosystems that supply

[56] Andrejevic, *Big Data Surveillance*.
[57] Fussey, *Command, Control and Contestation*.
[58] Samatas, *Surveillance in Athens 2004 and Beijing 2008*.

surveillance technology establish long-term relationships with governments; and the inter-agency protocols enhanced during Olympic planning can become templates for ordinary policing. Zuboff captured this phenomenon as being an infrastructural lock-in; once channels for capturing and monetising behavioural data are in place, strong incentives align to sustain them.[59] Authorities can point to gains in efficiency or safety, while companies emphasize innovation and cost-effectiveness. What begins as temporary necessity risks becoming permanent normality.

This drift has significant consequences. Principles such as due process, data protection, and proportionality can be cast aside, especially when predictive systems are treated as authoritative even though their inner workings are opaque. If a machine-learning model flags an individual or a crowd as "anomalous," the basis for that judgment is rarely transparent or contestable. Citizens may be subject to heightened scrutiny or intervention without ever knowing why, and without clear avenues for redress.

For scholars and policymakers, the key question is therefore not whether to use such tools, but under what conditions. What training data underlines the models, and how accurate are they across diverse populations? Who determines the thresholds that trigger alerts? What happens to people misclassified as threats? How long is data retained, and for what secondary uses? Who, beyond the technology vendors, can access it? These are not technical details but design and accountability choices that shape the balance between safety and civil liberty.

Comparative insight

Looking across Athens, Beijing, London, and Paris, a clear trajectory emerges in the evolution of Olympic surveillance. What began as optical watching through fixed CCTV cameras has gradually shifted towards cybersecurity, where algorithms process streams of data in real time. Surveillance has moved from post-hoc review, in which footage is analysed after the fact, to pre-emptive prediction, where alerts are generated before incidents unfold.

[59] Zuboff, *Surveillance Capitalism*.

Likewise, the human discretion of operators has given way to algorithmic triage, with machine outputs directing where attention and resources should flow.

The legal and political contexts of these Games differ, for example for the case of Athens and Beijing, they operated under a more centralised state model, London, on the other hand, within a liberal democracy concerned with terrorism, and finally Paris within the EU's stringent data-protection framework. Yet the underlying logics travel easily across borders. Hosts converge on similar promises: efficiency, safety, and innovation, all legitimised under the exceptional conditions of the Olympics.

Intellectual and academic debates are also something that has gone across borders. For example, scholars have highlighted the risks of data power and capture,[60] the way technical systems reorder social life,[61] the lock-in effects of surveillance infrastructures,[62] and, most recently, the specific dangers of AI video analytics in public space.[63] Taken together, these insights sketch a governance horizon in which prediction becomes policy, where decisions about risk and safety are increasingly shaped by algorithmic inference.

The Olympics play a central role in making this horizon feel both feasible and normal. By concentrating global attention, condensing political timelines, and framing security as an existential priority, they provide the perfect stage for surveillance innovations to be tested, displayed, and ultimately normalised. What begins as an Olympic experiment often becomes part of the everyday governance of the city.

C. Legal Oversight, Accountability, and Civil Liberties

[60] Andrejevic, *Big Data Surveillance*.
[61] Monahan, *Surveillance and Security.*
[62] Zuboff, *Surveillance Capitalism*.
[63] Zatsepina and Ludvigsen, *Algorithmic Olympics*.

Mega-events are composed of decision-making and the amplification of executive authority. The central legal problem is therefore not only "what extraordinary powers are granted", but "how those powers are bounded, supervised, and unwound once the event ends". Across literature and academic studies done on surveillance law, data protection, and security governance, scholars converged on a cautionary finding: without precise time limits, independent oversight, and effective remedies, "temporary" measures tend to stabilise into permanent structures.[64] [65] [66]

Doctrinal guardrails: necessity, proportionality, purpose limitation

Under the General Data Protection Regulation (GDPR), any restriction on fundamental rights must pass a strict and precise test. It must be *necessary*, meaning required for achieving a legitimate aim, not simply convenient. It must be *proportionate,* thus balanced against the scale of intrusion, ensuring that the measure does not exceed what is essential to mitigate the risk at hand. And finally, it must adhere to *purpose limitation*, the principle that data gathered for one clearly defined goal, such as Olympic crowd safety, cannot be repurposed for broader policing, intelligence, or even commercial uses without a new legal basis.[67]

The European Data Protection Board (EDPB) sharpened these expectations in its Guidelines 10/2020 on Article 23 GDPR, which deal explicitly with restrictions under emergency conditions. The Board insists that derogations from data-protection rights in such contexts must be targeted, time-bound, and reviewable.[68] This means that exceptional measures cannot be flexible; they must have a precise duration, subject to periodic review, and designed to expire once the emergency subsides. Furthermore, the EDPB requires transparency about scope and duration, so that both regulators and the public can see where the line between necessity and overreach is drawn.

---

[64] Paul De Hert and Serge Gutwirth, *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action* (2009).
[65] Graham Greenleaf, "Global Data Privacy Laws: 89 Countries, and Accelerating," *Queen Mary University of London, School of Law Legal Studies Research Paper* No. 98/2012 (2012).
[66] Samatas, "Security and Surveillance in the Athens 2004 Olympics," 225.
[67] European Union. *General Data Protection Regulation (GDPR).* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
[68] European Data Protection Board (EDPB), *Guidelines 10/2020 on Restrictions under Article 23 GDPR*, version 2.0, adopted October 13, 2021.

Certain case laws have reinforced these principles. For example, in Kennedy vs. United Kingdom, the European Court of Human Rights underscored that intrusive surveillance must rest on accessible law, ensuring that individuals can understand in advance the conditions under which they may be monitored. The Court also highlighted the need for independent authorisation and ongoing supervision, recognising that unchecked discretion in the hands of security agencies risks eroding fundamental rights.[69] These requirements are directly relevant to Olympic-time surveillance, where the scale and visibility of exceptional measures make the balance between security and liberty especially delicate.

Institutions that make (or break) oversight

Legal rights provide the formal guardrails for surveillance, but it is institutions that determine whether those rights are respected in practice. For example, in France, the Commission Nationale de l'Informatique et des Libertés (CNIL) played an unusually visible role before the start of Paris 2024. Its interventions on accreditation and laissez-passer systems highlighted the importance of data minimisation, strict retention limits, and access controls before large-scale deployments could proceed. By making its concerns public, the CNIL helped frame security not only as a matter of operational effectiveness but also of compliance with the rule of law.[70]

Oversight was not confined to privacy regulators. The Cour des Comptes, France's supreme audit institution, reminded Parliament that Olympic security was inseparable from questions of governance and legacy. Furthermore, a 2023 report highlighted weaknesses in inter-agency coordination and warned of the long-term risks associated with infrastructures built for temporary use.[71] Thus, the message was clear: financial integrity and data governance are two

[69] Kennedy v. United Kingdom, no. 26839/05, judgment of 18 May 2010, *European Court of Human Rights*, HUDOC item no. 001-98473,
[70] Commission nationale de l'informatique et des libertés, "Jeux olympiques et paralympiques 2024 : les observations de la CNIL sur le dispositif de laissez-passer," *CNIL*, May 13, 2024.
[71] Cour des comptes, *L'organisation des Jeux Olympiques et Paralympiques de Paris 2024: Rapport complémentaire au Parlement* (Paris: Cour des comptes, July 2023).

sides of the same accountability coin, and both must be scrutinised to prevent emergency measures from leaving unchecked legacies.

The British experience after London 2012 offers a parallel. The National Audit Office[72] and the House of Commons Committee of Public Accounts[73] examined Olympic security from a fiscal and performance point of view, exposing shortcomings in contracting and cost management, particularly after the G4S shortfall required military backfill. Meanwhile, the Home Affairs Committee[74] scrutinised capability gaps and blurred accountability lines between public and private actors. These inquiries did not only catalogue failings; they reinforced the principle that democratic oversight must remain active even when the language of "emergency" dominates public debate.

Taken together, these examples illustrate that oversight is best understood as a multi-layered ecology. Privacy regulators enforce data law, audit offices monitor spending and efficiency, and parliamentary committees exercise democratic scrutiny. Where such institutions are empowered, they can anchor Olympic security governance within a framework of legality and accountability. Where they are weak, however, paper rights risk being hollow, and exceptional measures may become normalised with little resistance.

Temporary law vs. permanent infrastructure

A recurring theme for academics is the uneasy relationship between temporary authorisations and the permanent infrastructures they leave behind. Samatas, wrote on Athens 2004 how emergency surveillance measures were initially framed as extraordinary but quietly adapted into long-term policing practice once the Games ended.[75] De Hert and Gutwirth described a parallel dynamic in European data-protection law, where once intrusive practices

[72] National Audit Office, *The London 2012 Olympic Games and Paralympic Games: Post-Games Review*, HC 794 (Session 2012–13), Report by the Comptroller and Auditor General, presented to Parliament on 5 December 2012, London: The Stationery Office, 2012.
[73] Committee of Public Accounts, *Post-Games review.*
[74] House of Commons Home Affairs Committee. *Olympics Security. Seventh Report of Session 2012–13, Volume I.* London: House of Commons, 2013.
[75] Samatas, *Security and Surveillance in the Athens 2004 Olympics*.

enter everyday administration, only important supra-national safeguards can rebalance the system.[76] On the other hand, Greenleaf broadens this perspective by indicating that as more countries adopt privacy statutes, mega-event surveillance increasingly collides with global compliance regimes, yet at the same time risks slipping into mission creep if purpose limitation is weak or poorly enforced.[77]

This tension is clearly visible in France's Law No. 2023-380, which authorised algorithmic video surveillance (AVS) for Paris 2024. While the law explicitly banned facial recognition and biometric processing, it permitted behavioural analytics, such as detecting crowd surges, abandoned luggage, or sudden movements, until March 2025, extending beyond the Games themselves.[78] Civil-society groups like Amnesty International France[79] and La Quadrature du Net[80] warned that even without facial recognition, such analytics amount to indirect profiling, subtly shifting surveillance from "*who people are to how they behave*". In practice, this blurs the line between event-time necessity and permanent behavioural governance.

The British experience after London 2012 illustrates how such legacies have unfolded in practice. Systems for accreditation, crowd monitoring, and transport telemetry, designed for Olympic-time risk management, were later absorbed into broader policing and urban management.[81] The lesson is that the end of the Games rarely coincides with the end of the infrastructures they generate.

The literature therefore emphasises that reversibility must be real, not symbolic. Sunset clauses should trigger the dismantling of infrastructures and deletion of data, not just perfunctory reviews that enable quiet extensions. Any continuation of Olympic-era systems must be justified through independent evaluation against necessity and proportionality standards, rather than operational convenience or claims of efficiency. Without such enforcement, temporary laws risk becoming Trojan horses through which emergency practices become normalised in everyday governance.

[76] De Hert and Gutwirth, *Data Protection in the Case Law.*
[77] Greenleaf, *Global Data Privacy Laws*.
[78] République française, *Loi n° 2023-380*, 20 mai 2023.
[79] Amnesty International France, *JO 2024 : Pourquoi la vidéosurveillance algorithmique pose problème*.
[80] La Quadrature du Net, *Algorithmic Video Surveillance, Dangers and Counter-attacks*.
[81] Fussey, *Command, Control and Contestation*.

Accountability in the algorithmic stack

As algorithmic video surveillance (AVS) and predictive tools become embedded in Olympic command centres, the issue of accountability moves from technical detail to constitutional principle. If an algorithm flags someone as "anomalous," who defines that threshold, and how can it be contested? Without clear safeguards, such systems risk shifting decisions of public order into opaque processes beyond democratic oversight.

Accountability must operate across the entire lifecycle of surveillance. Before deployment, rigorous DPIAs and transparent documentation of training data, error rates, and biases are needed to ensure necessity and proportionality. During operations, immutable audit logs, human-in-the-loop requirements, and independent monitors help keep algorithms advisory rather than determinative. Afterwards, public reporting on accuracy, strict data deletion, and accessible redress mechanisms are essential to prevent temporary measures from hardening into permanent infrastructures.

This multi-phase approach reflects Sloot and Koopmans, who stress ex ante authorisation, real-time supervision, and ex post auditing as a single chain of accountability.[82] It also aligns with the guidance of the UN Office of Counterterrorism[83] and INTERPOL's Project Stadia[84], as well as European analyses such as those by Statewatch[85], all of which emphasise proportionality, transparency, and reversibility. Ultimately, algorithmic security cannot be judged solely by its efficiency: it must remain subject to democratic checks that keep extraordinary powers truly exceptional.

[82] Sloot, Bart Custers, and Ruud Koopmans. "Ex Ante Authorisation, Real-Time Supervision, and Ex Post Auditing: Accountability in Algorithmic Governance." *Journal of European Public Policy* 28, no. 5 (2021): 761–780

[83] United Nations Office of Counterterrorism. 2021. *Guide on the Security of Major Sporting Events: Promoting Sustainable Security and Legacies.* Global Programme on the Security of Major Sporting Events. New York: UNOCT, June.

[84] INTERPOL. *Project STADIA: Executive Guidance for Major Event Security*. Lyon: INTERPOL, 2023.

[85] Statewatch, *Security of the Spectacle: The EU's Guidelines for Security at Major Events*, Analysis No. 207 (Brussels: Statewatch, December 2012), pp 36.

Contracts, vendors, and the G4S lesson

Oversight in mega-event security is not only a matter of constitutional safeguards; it is also profoundly contractual. The London 2012 Games offered an absolute reminder of this when the private security firm G4S failed to deliver the contracted number of guards, forcing the government to deploy military personnel on a short notice and all across the city of London. What began as a logistical lapse quickly became a parliamentary case study in opaque contracting, inadequate contingency planning, and blurred accountability lines.[86] [87] The episode revealed that vendor relationships are not just operational details but critical governance questions: when contractors falter, the state bears the political cost, and the boundaries of responsibility become contested.

The G4S case has since become a touchstone for discussions of procurement in security governance. Reviews of London 2012 stressed the need for clearer specifications, enforceable performance indicators, and stronger contractual levers to prevent similar failures.[88] [89] Scholars and oversight bodies alike suggest that effective procurement should go further, embedding open-book audit rights that grant regulators and auditors access to key operational data, including, in the age of algorithmic surveillance, the training sets, thresholds, and error profiles that determine how models classify risk. Contracts should also mandate independent accuracy and impact evaluations, making performance and rights implications measurable deliverables rather than afterthoughts. Clauses allowing systems to be switched off or scaled back if they cross rights thresholds are another safeguard, ensuring that procurement does not create a one-way path to permanent surveillance.

Without such levers, vendor ecosystems risk entrenching a form of technical and legal lock-in. As Zuboff has warned, infrastructures once built tend to persist, reinforced by commercial incentives and claims of efficiency.[90] This dynamic has been amplified through AVS, where proprietary systems shape frontline decision-making but are often shielded from scrutiny by

[86] Committee of Public Accounts, *Post-Games review.*
[87] Hopkins, Gibson, and Mulholland, *G4S Faces Financial Penalties*.
[88] National Audit Office, *Post-Games Review.*
[89] Committee of Public Accounts, *Post-Games review.*
[90] Zuboff, *Surveillance Capitalism.*

intellectual property protections. When key aspects of public safety are mediated by vendor-controlled algorithms, oversight becomes doubly complex: the state is not only supervising its own agencies but also navigating contractual asymmetries with private firms.

The lesson of G4S is therefore broader than one company's failure. It underscores that procurement is governance: the terms written into contracts determine whether Olympic security systems can be audited, corrected, or dismantled when they infringe on rights. In the absence of rigorous procurement frameworks, states risk ceding both operational control and democratic accountability to private actors, embedding exceptional security measures long after the Games have ended.

Host-city promises and supranational backstops

The governance of Olympic security is shaped not only by domestic law but also by contractual and supranational commitments that frame what is permissible. Since 2017, the IOC Host City Contract has embedded explicit references to human rights, raising the normative floor for security planning and signalling that hosts must balance safety with fundamental rights.[91] This marks a departure from earlier contracts, such as London's in 2005, which contained no comparable obligations. In practice, however, the enforceability of these provisions depends heavily on national and regional oversight institutions.[92]

National counter-terrorism frameworks provide the outer limits of lawful power. For London 2012, the UK's Counter-Terrorism Act 2008 and the CONTEST strategy authorised enhanced policing and surveillance powers, including pre-emptive monitoring.[93] In France, Plan Vigipirate continues to serve as the flexible legal and operational framework underpinning Paris 2024 security, adapting alert levels to threat assessments.[94] These frameworks allow rapid

[91] Comité International Olympique. *Contrat Ville Hôte – Principes, Jeux de la XXXIIIe Olympiade en 2024*, signed in Lima on 13 September 2017.
[92] International Olympic Committee, *Host City Contract for the Games of the XXX Olympiad in 2012*, executed in Singapore on 6 July 2005.
[93] United Kingdom, *London 2012 Olympic and Paralympic Safety and Security Strategy*, March 2011.
[94] *"Le plan VIGIPIRATE," Direction Générale de la Sécurité Intérieure (DGSI)*, published June 11, 2022 ; updated November 26, 2024.

mobilisation of extraordinary resources but also risk extending exceptional measures into ordinary governance if not carefully limited.

At the supranational level, additional checks exist. Following the 2015 Paris attacks, the FRA (European Union Agency for Fundamental Rights) warned against enduring states of emergency, stressing the importance of proportionality and reversibility.[95] Meanwhile, Europol and the EEAS (European External Action Service) integrated disinformation and cyber threats into their programming, showing how supranational actors can expand the security agenda without abandoning legal standards.[96] In France, VIGINUM and the SGDSN exemplified transparency by publishing open reports on information manipulation threats linked to Paris 2024, a practice that could, in principle, be extended to algorithmic surveillance and physical security infrastructures.[97]

Taken together, these layers illustrate the value of multi-tiered oversight. The IOC contract sets international expectations, national counter-terrorism frameworks define operational scope, and supranational institutions provide independent guardrails. No single layer is sufficient on its own, but in combination they increase the likelihood that emergency measures remain anchored in legality, time-bound, and subject to democratic control. In the Olympic context, where pressures for exceptionalism are strong, this layered model may be the most effective way to ensure that extraordinary security does not quietly become ordinary governance.

D. Public Trust, Media Framing, and Democratic Legitimacy

[95] European Union Agency for Fundamental Rights (FRA), *Reactions to the Paris Attacks in the EU: Fundamental Rights Considerations*, FRA Paper 01/2015 (Luxembourg: Publications Office of the European Union, 12 February 2015).
[96] European External Action Service, *Third EEAS Report on Foreign Information Manipulation and Interference Threats: Exposing the Architecture of FIMI Operations*, March 2025, European External Action Service.
[97] Secrétariat général de la Défense et de la Sécurité nationale (SGDSN), *Summary of the Information Threat to the Paris 2024 Olympic and Paralympic Games*, Public Report, September 19, 2024.

Olympic security is not only about gates, scanners, or algorithms, it is about how people actually live and feel those decisions. For spectators, security is experienced in the body: the long wait in line, the bag search, the sight of soldiers in a train station, or the quiet knowledge that cameras are watching. These encounters can feel reassuring, even part of the shared ritual of hosting the world. But they can also feel heavy, intrusive, and out of place. How the public interprets them depends not just on what is done, but on the stories surrounding them, whether the media frames them as necessary, excessive, or even theatrical. Trust, in this sense, is fragile. It must be earned not only through competence but through transparency and respect, and it can just as easily be lost when security seems more about spectacle than protection.

Security theatre and the experience of risk

For ordinary spectators, security is not experienced in the abstract language of "risk frameworks" but in the material textures of everyday movement: queues at checkpoints, armed soldiers patrolling train stations, bag searches at venues, drones overhead, or, more recently, cameras running algorithmic analysis. These are embodied encounters that make security feel either reassuring or oppressive. Consent to such measures is never absolute. It disappears and flows depending on how visible controls are, how intrusive they feel, and whether they appear justified.

As Giulianotti and Klauser argued, mega-events often generate a civic mood of collective duty, where inconvenience is now seen as part of the honour of hosting the world.[98] Standing in line or passing through scanners can become ritualised performances of participation in the Olympic project. Yet this delicate balance can tip into what critics call security theatre, visible displays of power that prioritise optics over effectiveness. Crilley, analysing London 2012, describes how rooftop missile batteries, naval ships on the Thames, and mass troop deployments created the impression of a militarised city, reassuring some citizens but on the other hand profoundly

[98] Richard Giulianotti and Francisco Klauser, "Security Governance and Sport Mega-Events: Toward an Interdisciplinary Research Agenda," *Journal of Sport and Social Issues* 34, no. 1 (2010): 49–61.

unsettling others.[99] What is meant to reassure can, in excess, signal insecurity and trigger protest.

Historical memory also weighs heavily on these dynamics. The Munich massacre of 1972 remains a recurring reference point, mobilised by organisers to legitimise exceptional vigilance at opening ceremonies and other symbolic moments.[100] Bellavita similarly noted that "special event security" operates in a climate of experienced trauma, where past attacks justify expansive, even experimental, measures.[101] For many citizens, this makes extraordinary precautions feel self-evident; for others, the repetition of emergency logics begins to normalise exception as routine.

The result is neither simple acceptance nor outright resistance, but an ongoing negotiation of necessity. People may tolerate bag searches if they believe the measure are truly necessary however, they will resent surveillance drones if they seem excessive or invasive. They may view soldiers on patrol as symbols of safety in the wake of terrorist threats yet be hesitant to the idea of algorithmic anomaly detection quietly monitoring their movements. What counts as "necessary" is therefore not fixed but constantly contested, shaped by media narratives, political framing, and lived experience on the ground.

Media narratives and the making of legitimacy

If publics experience security on the ground, they also interpret it through the prism of media narratives. The press, television, and, more recently, digital and social platforms do not simply report Olympic security; they frame it, translating queues, patrols, and surveillance into stories of reassurance, resilience, or controversy. These stories matter because they help shape whether extraordinary measures are seen as legitimate, excessive, or even theatrical.

---

[99] Rhys Crilley, "Urban Militarisation and the 2012 London Olympics," *E-International Relations*, July 2012.
[100] Bernhard Blumenau, *The Munich Massacre and Its Aftermath: A Securitization of Mega-Events*, Fondation Pierre du Bois Report No. 8 (Pully, Switzerland: Fondation Pierre du Bois, October 2022).
[101] Christopher Bellavita, "Changing Homeland Security: A Strategic Logic of Special Event Security," *Homeland Security Affairs* 3, no. 3 (2007).

Academic studies of London 2012 have revealed how celebratory narratives dominated much of the coverage. Vincent, Hill and Billings showed that British newspapers consistently recoded disruption as national pride: long queues became part of the collective sacrifice of hosting the world, and visible police presence was framed as evidence of Britain's organisational excellence.[102] Zhou and Zhong extend this analysis, describing how the Games were twisted into a project of "competitive identity," where narratives of security merged with narratives of Britain's global prestige.[103] Even language patterns reveal this blending. McEnery, Potts and Xiao found that reassurance and risk were linguistically braided, allowing security challenges to be narrated not as threats but as tests Britain had successfully passed.[104]

This framing had tangible effects. Research on residents showed that supportive media cues correlated with higher local acceptance of intrusive security controls.[105] When the media cast security as a civic contribution rather than a burden, publics were more inclined to interpret inconvenience as necessary and even honourable.

Yet counter-frames were equally vivid. The rooftop missile deployments, the use of the Royal Navy on the Thames, and the mass mobilisation of troops were widely covered, not just as measures of safety but as symbols of militarisation.[106] The G4S shortfall, in which the private security contractor failed to supply sufficient personnel, became a media spectacle in its own right, reported as a crisis of competence and governance.[107] [108] These episodes disrupted the celebratory script, fuelling scepticism and protest by portraying security as excessive, mismanaged, or driven by optics rather than need.

Taken together, the scholarship suggests that legitimacy is mediated: it does not flow automatically from the deployment of resources, but from the stories that accompany them. It

---

[102] John Vincent, John S. Hill, Andrew Billings, John Harris, and C. Dwayne Massey, "'We Are GREAT Britain': British Newspaper Narratives during the London 2012 Olympic Games," *International Review for the Sociology of Sport* 53, no. 8 (2018): 895–915

[103] Shuhua Zhou, Bin Shen, Cui Zhang, and Xin Zhong, *"Creating a Competitive Identity: Public Diplomacy in the London Olympics and Media Portrayal," Mass Communication and Society* 16, no. 6 (November 2013): 869–887.

[104] Tony McEnery, Amanda Potts, and Richard Xiao, *London 2012 Games Media Impact Study* (Lancaster: ESRC Centre for Corpus Approaches to Social Science, Lancaster University, 2012).

[105] Brent W. Ritchie, Richard Shipway, and P. Monica Chien, "The Role of the Media in Influencing Residents' Support for the 2012 Olympic Games," *Event Management* 14, no. 1 (2010): 1–14.

[106] Crilley, "Urban Militarisation and the 2012 London Olympics."

[107] Hopkins, Gibson, and Mulholland, "G4S Faces Financial Penalties."

[108] Rupert Neate, "G4S Profits Tumble on Olympics Failings," *The Guardian,* March 13, 2013.

rises when visible power is coupled with transparent rationale, when publics are told not just *what* is being done, but *why* it matters. It collapses when spectacle appears unmoored from proof, when the performance of security outpaces its justification. In this sense, the media act as both amplifiers and critics, capable of stabilising trust in Olympic security or of turning it into a lightning rod for discontent.

Generational trust gaps and protest politics

Trust in Olympic security is not evenly distributed across the public. It varies across generations, social groups, and lived experiences of policing. Ethnographic and policing research highlights that legitimacy is not produced in abstract strategies but in street-level encounters, the way stewards interact with crowds, how protests are handled, and how marginalised groups are treated in spaces of heightened surveillance.[109] A smile at a checkpoint or a heavy-handed dispersal can leave longer impressions on legitimacy than official press releases.

Generational divides are particularly striking. Publics shaped by the post-9/11 environment and the trauma of the 7/7 London bombings often see robust and massive security measures as common sense and completely normal, an expected part of urban life during global spectacles.[110] For these groups, visible armed patrols or intensive screening signal reassurance. By contrast, younger, digitally literate audiences, socialised in debates around privacy, surveillance capitalism, and data rights, tend to be more sceptical of experimentation with algorithmic tools or the indefinite storage of personal data.[111] For them, the Games are not only about sport but about the creeping normalisation of surveillance under the guise of festivity.

These divergences become especially visible in the arena of protest politics. Mega-events often reclassify dissent as disruption, securitising protest in the name of public order and spectacle.[112]

[109] Fussey, "Command, Control and Contestation".
[110] Boyle and Haggerty, "Planning for the Worst".
[111] Barrie Houlihan and Richard Giulianotti, "Politics and the London 2012 Olympics: The (In)Security Games," *International Affairs* 88, no. 4 (2012): 701–17.
[112] Giulianotti and Klauser, "Security Governance and Sport Mega-Events."

Demonstrations against militarisation in London 2012, or civil-society critiques of algorithmic surveillance in Paris 2024, illustrate how opposition to security measures can itself become a security concern. The paradox is clear: a celebration marketed as universal can simultaneously narrow the democratic space for disagreement.

The durability of public consent depends on how authorities manage this tension. When policing is procedurally just, transparent in rules, proportionate in interventions, and respectful in tone, resistance can soften, and publics may accept inconvenience as the price of safety. But when force is excessive, rules to intense, or dissent stifled, distrust spreads rapidly, especially in an era where social media instantly amplifies perceived injustices. In this way, generational sensibilities and protest politics together shape not just how security is enforced, but how it is remembered once the Games are over.

The algorithmic turn and the credibility problem

The arrival of AI-assisted video analytics has shifted the terrain of Olympic security from watching to sensing and predicting. Whereas CCTV once depended on human operators scanning screens, today's systems use models to classify behaviours in real time, labelling movements, gestures, or crowd flows as "normal" or "abnormal." As Dal Bello, Hirsch-Hoefler and Canetti observed, this reframes the very threshold of intervention: the trigger for action is no longer human recognition but algorithmic inference.[113] This makes the technology appear more objective, yet in practice it relocates discretion into code, into training data, model thresholds, and anomaly definitions that remain largely invisible to the public.

Paris 2024 became a focal point for this algorithmic turn. Law No. 2023-380 authorised the experimental deployment of algorithmic video surveillance, emphasising strict time limits, the exclusion of facial recognition, and a narrow list of predefined scenarios such as abandoned luggage or unusual crowd movements.[114] Officials presented this as a carefully bounded,

[113] Giulia Dal Bello, Sivan Hirsch-Hoefler, and Daphna Canetti, "AI Video Surveillance at the 2024 Paris Olympics," *The Loop*, September 24, 2024,
[114] République française, *Loi n° 2023-380*, 20 mai 2023.

temporary measure, security modernised without biometrics. Yet critics, including Amnesty International France [115] and La Quadrature du Net, [116] warned that even without facial recognition, behavioural profiling risks constructing indirect categories of suspicion. The worry was not only about the Games themselves but about post-Games normalisation: that temporary systems, once built and routinised, rarely disappear.

This is why the credibility problem looms so large. In algorithmic governance, legitimacy is not won by promises alone but by transparency. Publics increasingly expect concrete evidence: error rates, independent audits, and clear "sunset" mechanisms that guarantee decommissioning rather than quiet extension. Explainability and contestability are not technical luxuries; they are the democratic price of admission. Without them, opacity reads as unaccountable power, an unseen system that decides who or what counts as risky.

The lesson from Paris 2024 is that prediction itself must be governed. Trust depends less on the claim that systems are innovative, and more on whether they can be independently evaluated, limited in scope, and reversed when their mandate expires. Where that credibility is lacking, algorithmic surveillance risks being perceived not as reassurance but as yet another layer of security theatre, powerful, opaque, and resistant to democratic scrutiny.

Comparative lessons and practical implications

Looking across the recent Olympic cycles, from Athens 2004 to Paris 2024, a clear trajectory emerges in both technologies and public reactions. Each host city became laboratories of security, but publics also learned to interpret and judge these experiments. In Athens and Beijing, the dense deployment of cameras, centralised command rooms, and intelligence-sharing networks triggered fears of permanence. What was presented as temporary

[115] Amnesty International France, *JO 2024 : Pourquoi la vidéosurveillance algorithmique pose problème*.
[116] La Quadrature du Net, *Algorithmic Video Surveillance, Dangers and Counter-attacks*.

for the Games often appeared to linger afterwards, reinforcing anxieties that mega-event infrastructures rarely vanish when the crowds do.[117] [118] [119]

London 2012 shifted the debate toward trust in procurement and capacity. The G4S shortfall, where a private contractor failed to deliver promised personnel, turned security into a governance scandal as much as a technical one. Military backfill kept the Games safe, but the reputational damage endured: security was now judged not only on visibility but also on competence and accountability.[120]

Paris 2024 brought the conversation into the algorithmic age. Here, the central issue was no longer how many guards or cameras were visible, but whether algorithmic surveillance could be trusted, whether it was genuinely temporary, whether its error rates could be verified, and whether its legal sunset clauses would actually hold. Civil-society critiques underlined a growing public sophistication: people increasingly understand that promises of "no biometrics" do not end the debate if behavioural profiling persists and reversibility remains uncertain.

The lesson is simple but demanding when safeguards, stories, and street-level practice align, publics will often accept the burdens of exceptional security as part of the Olympic moment. When they diverge meaning when spectacle feels unmoored from necessity, or when reversibility is cast into doubt, the Games risk becoming less a festival of sport than a referendum on emergency power.

[117] Samatas, *Security and Surveillance in the Athens 2004 Olympics*.
[118] Samatas, *Surveillance in Athens 2004 and Beijing 2008*.
[119] Yu, Hai, Francisco Klauser, and Kin-Man Chan. "Governing Security at the 2008 Beijing Olympics." *The International Journal of the History of Sport* 26, no. 3 (2009): 390–405.
[120] Fussey, *Command, Control and Contestation*.

Part II – Security Systems in Context

This second part will examine how Olympic security took shape on the ground in London 2012 and Paris 2024, and how threat framing guided those choices. In London, the shadow of 7/7 produced a layered, intelligence-led model built on inter-agency coordination, private sector reliance, and highly visible deterrence. In Paris, the memory of 2015 and new hybrid risks, terrorism, cyber threats, civil unrest, pushed authorities toward legal innovation and the experimental use of algorithmic video surveillance, assessed most visibly during the open-air ceremony on the Seine. Beyond operations, the focus here is on what these systems meant for legitimacy: whether oversight was effective, whether sunset clauses were held, and whether publics felt protected or controlled once the Games were over.

A. London 2012: Context and Approaches

When London won the right to host the 2012 Olympics, the city was still celebrating when tragedy struck the very next day: the 7/7 bombings on its transport system. That moment changed everything. The Games were no longer just about sport, pride, or spectacle, they were also about proving that London could be safe, resilient, and united in the face of fear. Planning for 2012 became as much about protecting people as about welcoming them, weaving security into the very fabric of the event. In numerous ways, the Olympics became a test: could a city keep millions safe without losing the joy and openness the Games were meant to inspire?

Terrorism Concerns

The planning for the London 2012 Olympic and Paralympic Games was profoundly shaped by the traumatic events of July 7th, 2005, when a series of coordinated suicide bombings on London's public transport system claimed the lives of 52 civilians and

injured 784 others.[121] These attacks were carried out by four British born Islamist extremists, Hasib Hussain, Mohammad Sidique Khan, Germaine Lindsay and Shehzad Tanweer, therefore highlighting the need for the British government to prioritize counter-terrorism measures in its Olympic planning, focusing on surveillance, intelligence gathering, and public safety initiatives. Importantly, these attacks occurred just a day after the 117th International Olympic Committee Session in Singapore where the city of London won, against Paris, the bid to become the host city for the 2012 Summer Olympics and Paralympics Games, thus immediately transforming the Games into a symbol of national resilience and a potential terrorist target.[122]

In March 2011, the Home Office's Olympic and Paralympic Safety and Security Strategy outlined a layered, risk-based approach to preventing terrorism and safeguarding the Games. This approach combined proactive deterrence with resilience-building, incorporating both visible and invisible security measures. Key elements included the deployment of advanced surveillance technologies, biometric accreditation systems for staff and athletes, enhanced perimeter controls, and integrated threat assessments shared across a network of law enforcement, intelligence services, and emergency responders.[123] This multi-agency coordination was structured around the OSSSRA and Risk Mitigation Process, which served as the core framework for evaluating both high and low-probability threats. This strategy enabled planners to dynamically adjust their security posture in response to real-time intelligence, ensuring the flexibility required for a complex and high-profile international event.[124]

In the aftermath of the 7 July 2005 London bombings, the British government undertook a significant reassessment of its counter-terrorism apparatus. Central to this effort was the publication of the Government Response to the Intelligence and Security Committee's (ISC) Report into the London Terrorist Attacks, which was released in May 2006. This official response confirmed many of the ISC's findings, including several critical shortcomings in intelligence handling and inter-agency coordination that preceded the attacks. A major concern raised in the ISC's report, and acknowledged by the government, was the fact that two of the suicide bombers, Mohammad Sidique Khan and Shehzad Tanweer, had already come to the attention of the security services prior to the bombings. Both individuals had appeared in surveillance

[121] British Transport Police, "London Bombings of 2005," *British Transport Police*, 2023.
[122] The Guardian. *The Party That Never Was: Capital Marks the Games at Last*. September 2, 2005.
[123] United Kingdom, *London 2012 Olympic and Paralympic Safety and Security Strategy*, March 2011.
[124] Home Office, *OSSSRA Summary, Version 2.*

operations linked to other investigations, yet they were not prioritized for further scrutiny. The government's response cited limited investigative resources and competing priorities at the time, which led to the de-prioritisation of both suspects despite their appearance in existing intelligence streams.[125]

The report also exposed a more systemic issue: the failure to adequately identify and assess the threat posed by individuals engaged in known extremist networks. Khan and Tanweer were not wholly unknown entities; their names surfaced in operations that involved individuals later convicted of terrorist offences. However, they were assessed as non-dangerous figures, and their profiles were not developed further, an error the government recognized as a failure in both threat assessment and risk prioritization.

Perhaps most critically, the ISC's report, and the government's subsequent response, highlighted longstanding weaknesses in inter-agency communication and coordination. While there were multiple agencies involved in the broader counter-terrorism landscape, including MI5, the police, and regional intelligence bodies, their efforts were not consistently synchronized. This fragmentation led to missed opportunities for intelligence sharing, which might have allowed for more comprehensive assessments of the suspects' activities and affiliations.

In response, the British government committed to a series of institutional and operational reforms. These included strengthening MI5's domestic intelligence capabilities, increasing investment in surveillance and analytical resources, and most notably, establishing Regional Counter-Terrorism Units (RCTUs) designed to enhance multi-agency collaboration at the local level. The report also emphasized the importance of creating clearer protocols for the joint management of intelligence, a move that would later underpin the development of the UK's integrated CONTEST strategy.

The 7/7 attacks also catalysed a conceptual shift in counterterrorism thinking. Before 2005, British counter-terrorism policy was largely centred on external threats, particularly large-scale plots orchestrated by transnational organizations such as al-Qaeda.[126] The London bombings forced a recognition that the most pressing threat could originate from within: homegrown radicalization, operating through informal networks or even in complete isolation. As

[125] UK Government. *Government Response to the Intelligence and Security Committee's Report into the London Terrorist Attacks on 7 July 2005.* May 2006.
[126] Fussey, *Command, Control and Contestation*.

acknowledged in the *Countering International Terrorism* strategy, the 7/7 attackers were British citizens who had been radicalized within the UK, acting independently and without direct operational links to any central terrorist organization.[127] This reframing of the threat environment necessitated not only enhanced technical surveillance, but also more proactive community engagement, educational outreach, and pre-emptive interventions.

To address these challenges, the *CONTEST* strategy introduced the *PREVENT* pillar, aimed at stopping individuals from becoming terrorists in the first place. This included investments in counter-radicalization programs, partnerships with schools and religious leaders, and new efforts to combat online extremism. The rise of the so-called "lone wolf" terrorist, individuals who may act without formal affiliations but are ideologically driven and capable of devastating violence, emerged as a core concern.[128] This model of terrorism disrupted traditional intelligence methods, which were structured to identify coordinated plots rather than ideologically motivated individuals acting independently. This highlights how pre-7/7 intelligence structures were ill-equipped to manage this more amorphous threat, prompting the institutional reforms that followed.[129]

London 2012 was thus not only about preparing for spectacular attacks in the Mold of 9/11 or Madrid, but also about building resilience against domestically radicalized individuals operating under the radar. This was reflected in multi-layered security planning that combined high-visibility policing with behind-the-scenes intelligence fusion and behavioural threat detection. Public awareness campaigns also played a critical role, encouraging citizens to report suspicious behaviour as part of a wider civic engagement in security.

These lessons would echo far beyond the UK. For example, the emerging threats facing the 2024 Paris Summer Olympics and Paralympics Games. Western democracies continue to face the persistent danger of small cells and lone actors, often radicalized online and embedded within national borders. The British experience with London 2012, particularly its pivot toward pre-emptive, community-based, and multi-agency approaches to domestic terrorism, has become a reference point in global Olympic security doctrine. In this sense, London 2012 marked not only

[127] UK Government, *Response to ISC Report on 7 July 2005 Attacks.*
[128] Home Office. *Countering International Terrorism: The United Kingdom's Strategy.* London: Home Office, 2006.
[129] Kevin J. Strom and Joe Eyerman, "Interagency Coordination: Lessons Learned From the 2005 London Train Bombings," *NIJ Journal*, no. 261 (July 2008), 28–32.

a test of technical resilience but a turning point in the global understanding of terrorism in the age of hybridized, internalized threats.[130]

Inter-agency Coordination

To manage the extensive security requirements of the London Olympics, the United Kingdom adopted a centralized and collaborative model of governance. To answer this objective, the Olympic Security Directorate (OSD) was formed, thus bringing together multiple agencies including MI5, the Home Office, the Metropolitan Police Service, the British Transport Police, and the Ministry of Defence. The objective was to establish a unified structure that could respond swiftly, thereby enhancing coordination among agencies and enabling effective management of a broad range of threats. This effort included the creation of the London 2012 OSSSRA and Risk Mitigation Process, a document that would continuously track evolving risks and updated daily operational decisions. This coordination would not only be confined inside Britain's borders but also beyond, involving cooperation with international partners such as the FBI, Europol, and Interpol.[131] These partnerships were essential for intelligence sharing, especially in relation to transnational threats. Joint training exercises, inter-agency briefings, and simulation drills were conducted regularly to enhance preparedness and ensure all actors understood their roles in case of emergency.

A defining feature of the London 2012 Olympic and Paralympic Games was the unprecedented scale and complexity of its security operation, described by the UK police as the largest pre-planned policing effort in British history.[132] At the heart of this effort was a multi-layered system of inter-agency coordination, developed in response to the intelligence failures that preceded the 7 July 2005 London bombings. As highlighted in the Government Response to the Intelligence and Security Committee's Report into the London Terrorist Attacks,[133] a key failure

[130] Petter Nesser and Wassim Nasr, "The Threat Matrix Facing the Paris Olympics," *CTC Sentinel* 17, no. 6 (June 2024).
[131] United Kingdom, *London 2012 Olympic and Paralympic Safety and Security Strategy*, March 2011.
[132] National Police Chiefs' Council, *Police Service Delivers Resources for Largest Ever Pre-Planned Operation: The London 2012 Olympic and Paralympic Games*, press release, May 21, 2012.
[133] UK Government, *Response to ISC Report.*

on 7/7 was the fragmentation between MI5, local police forces, and intelligence units, which had failed to detect and act upon signals from individuals like Mohammad Sidique Khan.

The restructuration of British counterterrorism after the 7/7 London bombings placed a strong emphasis on coordinated, multi-agency frameworks, and as a result the 2012 Olympic Games served as a real-world test of these frameworks. The creation of the Olympic Security Directorate (OSD), within the Metropolitan Police, is seen as one of the creations that had a major influence on the well-being of the event. The OSD was tasked with overseeing all aspects of Olympic security coordination, serving as the operational hub for strategic planning, inter-agency integration, and command and control during the Games. It was led by Assistant Commissioner Chris Allison, who functioned as the National Olympic Security Coordinator, ensuring alignment among all UK police forces, the Home Office, intelligence agencies, and international partners.[134]

The OSD managed the integration of over 100 public and private organizations.[135] Key actors included the Home Office, MI5, the Cabinet Office, the Department for Transport, Transport for London, UK Border Agency, the British Transport Police, and all police forces in host venues. The National Olympic Coordination Centre centralized coordination across the United Kingdom and operated around the clock, facilitating real-time decision-making and intelligence flow.[136]

Furthermore, the Games also innovated in inter-agency planning for public health and safety, expanding coordination beyond traditional security actors to include the NHS, the Health Protection Agency, and London Ambulance Service. This broader model ensured that mass casualty preparedness, public health surveillance, and biohazard response were fully integrated into the overarching Olympic security plan.[137] According to the London 2012 Official Report, this resulted in over 200 joint exercises and simulations conducted in the run-up to the Games, testing the interoperability and readiness of both civilian and uniformed responders.[138]

---

[134] NPCC, *Police Service Delivers Resources for Largest Ever Pre-Planned Operation*.
[135] United Kingdom, *London 2012 Olympic and Paralympic Safety and Security Strategy*, March 2011.
[136] Mark Scoular. *Multi-Agency Response Capabilities and Planning for Significant Sporting Events*. Josoor Institute, 2021.
[137] Angeliki Bistaraki, Eammon McKeown, and Ioanna Kyratsis, "Systems Readiness and Crisis Leadership during London 2012," *Public Health* 165 (2018): 119–26.
[138] London Organising Committee of the Olympic Games and Paralympic Games (LOCOG), *London 2012: Official Report, Volume 3 – Servicing the Games* (Lausanne: IOC, 2013).

From a tactical standpoint, information fusion was essential as there was a need to learn from the mistakes of the 7/7 Bombings where the lack of integrated threat monitoring had allowed relevant intelligence to remain siloed. In contrast, by 2012, joint intelligence operations between MI5, SO15 (the Metropolitan Police Counter Terrorism Command), and JTAC (Joint Terrorism Analysis Centre) had become routine. Analysts and decision-makers were co-located within shared operations centres to support unified threat assessments. These hubs enhanced the speed and clarity of operational responses, particularly under fast-moving conditions such as suspicious packages or chemical threats.[139]

The OSSSRA served as the formalized framework underpinning inter-agency threat coordination. OSSSRA allowed agencies to work from a shared understanding of high- and low-probability risks, including terrorism, cyber threats, major protests, infrastructure disruption, and pandemics.[140] As highlighted by the London 2012: Protecting the Olympic Games report, this risk-based approach allowed for flexible resourcing and rapid escalation protocols that could be tailored to specific threat levels.

Despite these efforts, coordination between those actors and agencies was not without failures. For example, private security provider, G4S, failed to deliver enough trained personnel just weeks before the Games, thus forcing the government to deploy 3,500 additional military personnel to fill the gap.[141] While this emergency measure underscored the robustness of contingency planning, it also revealed tensions in public-private coordination within an otherwise highly synchronized system.

Ultimately, London 2012 demonstrated the sustainability of a deeply integrated, multi-agency security model grounded in both intelligence fusion and community-level resilience. These Games were intended to represent a moment of national celebration, but their real success would lay in the invisible infrastructure of coordination and preparedness that kept them

[139] Strom and Eyerman, *Interagency Coordination*.
[140] United Kingdom, *London 2012 Olympic and Paralympic Safety and Security Strategy*, March 2011.
[141] Hopkins, Gibson, and Mulholland, *G4S Faces Financial Penalties*.

safe.[142] These lessons now inform the planning of future Olympic security efforts, including Paris 2024, which has been heavily influenced by the London blueprint.[143]

Private Sector Involvement

One of the most contentious and revealing aspects of the London 2012 security framework was its deep and unprecedented reliance on private sector contractors. At the heart of this model stood G4S, the world's largest security services provider at the time, which was awarded a contract worth approximately £284 million to supply over 10,000 trained security personnel. These personnel were expected to undertake critical duties including perimeter surveillance, access control, and screening at Olympic venues. The partnership was intended to showcase a cost-effective, scalable model for public-private collaboration in the delivery of mega-event security. However, in the weeks leading up to the opening ceremony, it became apparent that G4S had failed dramatically to meet its contractual obligations as they did not recruit, vetted, or train enough personnel to fulfil their commitments, therefore exposing a massive operational gap just as the Games approached their most sensitive phase.[144]

This shortfall triggered a last-minute scramble within government circles, culminating in the emergency deployment of an additional 3,500 military personnel. These troops joined an already sizable contingent of 13,500 military staff assigned to Olympic duties, further militarizing the security landscape of the event.[145] This revelation provoked national outrage and widespread media condemnation. It also ignited a formal inquiry by the House of Commons Home Affairs Committee, which concluded that both G4S and the Home Office had gravely underestimated the complexity, logistical demands, and sensitivity of securing an international

[142] Andrew Culf, "The party that never was: capital marks the games at last," *The Guardian*, September 2, 2005.
[143] Nesser and Nasr, *Threat Matrix Facing the Paris Olympics*.
[144] *The Guardian. London 2012 Olympics: G4S Failures Prompt Further Military Deployment*. July 24, 2012.
[145] Hopkins, Gibson, and Mulholland, *G4S Faces Financial Penalties*.

event on the scale of the Olympics.[146] The committee pointed to systemic flaws in risk forecasting, project oversight, and contractor management.

Internally, G4S initiated its own review of the failure, which laid bare a range of structural and managerial deficiencies. According to the company's post-Games report,[147] several internal processes, including project management protocols, workforce recruitment timelines, and personnel tracking mechanisms, were not designed to meet the unique challenges of a mega-event. Miscommunication between teams, unrealistic recruitment benchmarks, and insufficient contingency planning were all cited as contributing factors to the collapse in delivery. The crisis reached its public climax when G4Ss CEO Nick Buckles was summoned to testify before Parliament. During the hearing, Nick Buckles publicly apologized and announced he would forfeit his annual bonus. The reputational damage to the firm was immediate and severe, as its stock price fell and its credibility as a security provider was called into question.[148]

On the ground, the operational failures were even more visible. Reports emerged of inadequately trained recruits arriving at venues without clear instructions, uniforms, or understanding of their assigned responsibilities.[149] These accounts further eroded confidence in the ability of private contractors to uphold the lofty standards required for national and international security. The episode became emblematic of wider concerns about the increasing privatization of core state functions, particularly those as sensitive and symbolically charged as security. London 2012 epitomized the encroachment of market logics into the governance of mega-events. The commodification of public safety suggests risks prioritizing profitability and cost-efficiency over reliability and democratic accountability.[150]

From a policy and governance perspective, the G4S debacle underscored several key vulnerabilities in the hybrid public-private security model. One of the key issues surrounding this debacle was the lack of a robust and enforceable oversight mechanism. While the British Government had entered into the contract expecting G4S to deliver a turnkey solution, it failed

[146] House of Commons Home Affairs Committee. *Olympics Security: Seventh Report of Session 2012–13* (HC 531-I). London: The Stationery Office, published 21 September 2012, ordered printed 18 September 2012.
[147] G4S. *London 2012 Olympic and Paralympic Games: Post-Games Report.* London: G4S, 2012.
[148] Neate, *G4S profits tumble on Olympics failings*.
[149] Robert Booth and Nick Hopkins, "Olympic security chaos: depth of G4S security crisis revealed," *The Guardian*, July 13, 2012.
[150] Fussey, *Command, Control and Contestation*.

to implement sufficient monitoring procedures to verify recruitment progress or training standards in real time. This created a dangerous blind spot within the operational chain of command. The fallback to military reinforcement, while ultimately effective in maintaining security continuity, revealed the fragility of the contingency architecture and highlighted the risks associated with over-dependence on private entities without parallel public sector redundancies.

The UK Government's post-Games evaluation conceded that contractual oversight had been inadequate and that key assumptions underpinning the outsourcing strategy were flawed. The report stressed the importance of maintaining a strong core of public security forces and integrating private actors only with strict vetting procedures, enforceable accountability frameworks, and clear escalation protocols.[151] The G4S failure thus served as a vivid demonstration of how essential it is to embed resilience and flexibility into the structure of Olympic security planning, especially when relying on third-party providers.

For future Olympic host cities, including Paris 2024, the G4S case continues to serve as a powerful warning. French institutions have taken this lesson quite seriously as it was seen in a 2023 evaluation of the French Cour des Comptes where they explicitly referenced London 2012 as a case study illustrating the risks of inadequate procurement and oversight mechanisms. The French auditors recommended more rigorous vetting processes for private security providers, greater state-led supervision of implementation phases, and pre-planned contingency pathways to ensure operational redundancy in the event of a contractor failure.[152] In short, they urged a shift away from reliance on market self-regulation and towards a more interventionist state posture in managing the security of globally significant events.

What the G4S controversy revealed, beyond the failure of a single firm, was the fragility of an Olympic security architecture overly reliant on commercial outsourcing without sufficient public control. This unfortunate event forced the rethinking of assumptions that had underpinned public-private collaboration in event security for over a decade. While the incident did not ultimately compromise the safety or success of the London Games, it did have a reputational,

[151] UK Government. *The London 2012 Olympic Games and Paralympic Games: Post–Games Review, Fortieth Report of Session 2012–13.* London : The Stationery Office, 2013.
[152] Cour des comptes, *Rapport complémentaire au Parlement.*

logistical and financial cost on both the government and the contractor. More importantly, it generated critical momentum for post-event institutional learning and reform.

To conclude, the G4S incident provides a rich case study in the potential and downfalls of private sector engagement in Olympic security. It highlights the necessity of balancing efficiency and flexibility with rigorously maintained standards, transparent oversight, and robust fallback options. The incident serves as a reminder that while private firms may support security efforts, the ultimate responsibility for public safety at such events must remain with the state. Only through a carefully calibrated blend of public authority, contractual discipline, and operational readiness can host nations hope to avoid the kinds of breakdowns that nearly marred the London 2012 experience.

Public Perception and Media Discourse

Public perception of Olympic security efforts was shaped by both the visible presence of security personnel and extensive media coverage. The London 2012 Olympic and Paralympic Games marked not only a massive logistical and security undertaking but also a deeply symbolic contest over the meaning and visibility of security in public life. Public perception of the security arrangements was heavily influenced by the highly visible deployment of military assets across the capital, combined with intensive media scrutiny and competing political narratives. Even though the entirety of the event was mostly delivered without incidents, measures such as rooftop missile installations, armed patrols, and military vehicles stationed around London led to concerns about the 'militarisation' of public space. While some citizens appreciated the sense of safety these measures conveyed, others viewed them as excessive and a threat to civil liberties.[153] This duality, wavering between reassurance and alarm, lay at the heart of the securitization debate surrounding London 2012.

Among the most controversial measures was the instalment of missile batteries on the top of civilian apartment buildings, including sites such as the Lexington Building in Bow and the Fred

[153] George, Richard, and Rob. I. Mawby. "Security at the 2012 London Olympics: Spectators' Perceptions of London as a Safe City." *Security Journal* 28, no. 1 (2013): 1–11.

Wigg Tower in Leytonstone.[154] Though rationalized by authorities as necessary responses to potential aerial threats, these installations became highly symbolic flashpoints. Critics, residents, and civil liberties advocates decried them as evidence of the creeping "militarization" of urban space.[155] Affected residents filed legal actions, and civil society organizations expressed concerns about the lack of transparency and public consultation. As a result, these developments contributed to a wider unease concerning the boundaries between public safety and state overreach, especially when military force became the visible guarantor of civic order.[156]

The image in the heads of London residents of soldiers patrolling London's streets, Royal Navy vessels moored along the Thames, and RAF jets on standby was widely disseminated in both domestic and international media. These outlets and medias would display messages that alternated between praising the readiness of security services and others questioning the suitability of turning the capital into what some commentators described as a "security fortress", and this would have a significant impact on the British and London population.[157] Some would even argue that the Games had transformed London into a showcase of "militarized neoliberal security," where exceptional measures were normalized under the banner of Olympic celebration.[158]

This dichotomy between reassurance and surveillance formed the heart of the securitization narrative. On the one hand, the governments accounts, particularly from the Home Office, emphasized the extraordinary scale of the Games and the corresponding need for extraordinary protection. This official communication strategy was calibrated in a way to reassure the public that the visible military presence was both temporary and essential for the well-being of those games.[159] As we have seen, this narrative was constructed to promote safety, resilience, and professionalism. Despite that, this messaging often coexisted uncomfortably with critical media framings that suggested a shift toward more permanent forms of security governance, what some have called the Olympic security-industrial complex.[160] [161]

---

[154] BBC News. *London 2012: Olympic Missiles Put in Position*. July 12, 2012.
[155] Crilley, *Urban Militarisation and the 2012 London Olympics*.
[156] George and Mawby, *Security at the 2012 London Olympics*.
[157] Houlihan and Giulianotti, *Politics and the London 2012 Olympics*.
[158] Crilley, *Urban Militarisation and the 2012 London Olympics*.
[159] United Kingdom, *London 2012 Olympic and Paralympic Safety and Security Strategy*, March 2011.
[160] Weijer, *Securitization and the London 2012 Olympic Games.*
[161] Fussey, *Command, Control and Contestation*.

However, public reaction was far from being uniform. While certain Londoners expressed pride in the UK's readiness and professionalism, others reported feelings of unease or alienation in their own neighbourhoods. The perceptions of security were shaped as much by emotion and personal ideology as by factual knowledge. While the majority felt reassured by the heavy security presence, a significant minority questioned its proportionality and raised concerns about its long-term implications for civil liberties.[162] This tension between perceived safety and perceived intrusion mirrored the debates that had emerged following the 2005 London bombings and the subsequent adoption of more robust counter-terrorism frameworks.[163] [164]

Despite those controversies, post-Games evaluations revealed important levels of public satisfaction with the overall security environment. Surveys conducted in the months following the event reported that a majority of attendees felt safe and supported during the Games, a testament to the operational success of the security apparatus.[165] However, this apparent success did not negate the lasting questions raised about the limits of state power, the symbolic use of military imagery, and the role of the media in framing these dynamics.

Furthermore, discourse from the media in particular played a decisive role in shaping public understanding and political reception of Olympic security. This is due to the fact that the British press oscillated between celebratory nationalism and critical introspection. While the dominant narrative in the tabloid press framed the Games as a triumph of British resolve and organizational excellence, broadsheet outlets and academic commentators highlighted issues of surveillance, exclusion, and the erosion of democratic norms in the name of national security.[166] These tensions were amplified by the international press, with several foreign commentators expressing unease at the visual spectacle of missiles in densely populated residential areas. From a historical and geopolitical point of view, the London 2012 Olympic and Paralympic Games security discourse cannot be separated from the legacy of earlier terrorism threats, including the 1972 Munich massacre and the 2005 London bombings. This shadow of Munich continues to influence and shape the Olympic security doctrine, embedding a culture of anticipation and exceptionalism in the planning process. London 2012 inherited this legacy,

[162] George and Mawby, *Security at the 2012 London Olympics*.
[163] Strom and Eyerman, *Interagency Coordination*.
[164] UK Government, *Response to ISC Report.*
[165] LOCOG, *London 2012 Official Report, Vol. 3*.
[166] Vincent et al., *'We Are GREAT Britain'*, 900.

translating it into a comprehensive security strategy that fused counterterrorism, public order, and spectacle into a singular, visible performance of state power.[167]

Looking ahead to Paris 2024, these debates retain sharp relevance. The French Cour des Comptes has explicitly drawn lessons from London's experience, warning French authorities about the dangers of excessive securitization and thus recommending greater transparency, public engagement, and legal safeguards.[168] The French government's use of AI-enhanced video surveillance, enabled by the controversial 2023 Olympic security law, has already sparked media concern over a potential slide toward mass surveillance.[169] As with London, the challenge for Paris will be to manage the complex interplay between visibility, reassurance, and rights in the construction of Olympic security space.

To conclude, the London 2012 Olympic and Paralympic Games offered a compelling case study in the tensions between security effectiveness, public perception, and democratic legitimacy. The visual and symbolic aspects of military and police presence transformed Olympic security from a background process into a public spectacle, one that inspired both confidence and criticism. While the event itself may have been secure, the long-term implications of the security approach continue to resonate in policy debates, media discourse, and the evolving architecture of mega-event governance.

B. Paris 2024: New Risks in a Shifting Landscape

The Paris 2024 Olympic and Paralympic Games unfolded in a world quite different from that of London 2012. France faced not only the lingering shadow of past terrorist attacks but also a web of new and unpredictable risks such as cyberwarfare, disinformation, and widespread civil unrest. Against this backdrop, security planning became more than a technical

[167] Blumenau, *Munich Massacre.*
[168] Weijer, *Securitization and the London 2012 Olympic Games.*
[169] O'Brien, *Paris 2024: French Government Approves Controversial AI Video Surveillance*.

exercise; it was a test of how a democracy balances openness and spectacle with vigilance and control. This section explores how Paris navigated this shifting landscape, from terrorism and hybrid threats to the unprecedented use of AI surveillance and the challenges of staging an open-air ceremony on the Seine.

Complex threat environment

The Paris 2024 Olympic and Paralympic Games took place in a significantly altered and multidimensional security context. Compared to previous Olympic host cities, particularly London 2012, Paris had to confront a far more unpredictable convergence of residue terrorist threats and emergent hybrid risks. The Games took place not just under the shadow of potential physical violence, but amid escalating concerns about cyber-disruption and warfare, disinformation, civil unrest, and the possible lack of public trust in state institutions. France's contemporary security challenges were profoundly rooted in recent national trauma and sociopolitical tensions, most notably the November 2015 terrorist attacks as well as the growing presence of civil disobedience and protest, comprising an important share of the French population.

The legacy of 2015, where quite a few terrorist attacks were coordinated in Paris, such as the Charlie Hebdo shooting that took place on the 7th of January, the Hyper Cacher kosher supermarket siege that took place on the 9th of January and finally the shootings that occurred across Paris on the 13th of November continued to shape both public perception and the institutional security doctrine. Claimed by the Islamic State, these attacks marked a seismic shift in the French state's counterterrorism approach. In their aftermath, France enacted extensive emergency powers, expanded domestic surveillance, and deployed the military across urban centres under Operation Sentinelle. These measures have since been embedded into national security law.[170]

The resonance of these attacks echoed that of Munich 1972, as this tragic incident is often seen as one and even the foundational trauma in the global securitization of mega-events. Thus, just

[170] Florence Faucher and Laurie Boussaguet, *"The Politics of Symbols: The French Government's Response to the 2015 Terrorist Attacks,"* Cogito (Sciences Po), October 27, 2018.

as Munich permanently altered how Olympic Games are protected, the terrorist attacks that stroke Paris in 2015 remained a "memory anchor" for French security planning.[171] During the organization of this mega-event and the securitization of each venue, jihadist terrorism, radicalized lone actors, as well as ideological domestic extremism were viewed as credible risks. The decentralized structure of the 2024 Games, with events across Paris, Marseille, Saint-Denis, and even Tahiti, complicated perimeter-based protection and escalated the symbolic appeal of the Games as a terrorist target.[172]

While terrorism remained a core concern, it was increasingly overshadowed by hybrid threats, such as cyberwarfare. Cybersecurity was among the most urgent priorities for Paris 2024 as the digitalization of Olympic operations, including ticketing systems, biometric accreditation, crowd monitoring, and AI-assisted surveillance, significantly expanded the attack surface for malicious actors.[173]

In its 2024 report, WithSecure[174] warned of coordinated cyber campaigns from both state-aligned and freelance hacktivist actors. These groups pursued geopolitical, ideological and anti-globalist objectives. In July 2024, French authorities confirmed that several cyber intrusions targeting Games-related systems had been thwarted.[175] Law N°2023-380 authorized preventive deployment of algorithmic surveillance as AI-assisted video analysis in public spaces and biometric recognition for crowd control. The use of such technologies was justified by the government as necessary adaptations to the scale and complexity of Olympic security needs.[176] However, this unprecedented use of algorithmic surveillance in such a complex democratic context sparked intense debate. Civil society organizations, digital rights advocates, and data protection authorities raised concerns over transparency, proportionality, and the absence of robust safeguards against abuse.[177] Many argued and still to this day that the deployment of such tools during a high-profile international event risks the normalization of intrusive

[171] Blumenau, *Munich Massacre.*
[172] Nesser and Nasr, *The Threat Matrix Facing the Paris Olympics*.
[173] Cour des comptes, *Rapport complémentaire au Parlement.*
[174] Tim West, *The Cyber Threat to Paris 2024 Olympics*, report (WithSecure: Intelligence & Foresight Unit, July 2024).
[175] Mike Elgan, "How Paris Olympic Authorities Battled Cyberattacks, and Won Gold," *IBM Think* (blog), August 23, 2024.
[176] République française, *Loi n° 2023-380*, 20 mai 2023.
[177] O'Brien, *Paris 2024: French Government Approves Controversial AI Video Surveillance*.

surveillance in everyday life, potentially setting a precedent for future large-scale events or domestic policing practices.

With cyberwarfare, disinformation and foreign information manipulation emerged as insidious and sinister risks to institutional legitimacy. The European External Action Service identified the Olympics as a high-value vector for foreign influence operations, warning of false security alerts, social media propaganda, and efforts to amplify domestic grievances. Such cognitive warfare aimed to destabilize societal trust in the French government and security apparatus.[178]

French authorities integrated disinformation monitoring into their security protocols, however the diffuse nature of these threats, blurring the lines between internal and external actors, made them uniquely difficult to contain. As seen during the COVID-19 pandemic, informational disturbance could undermine public morale and reduce compliance with emergency measures. Given the symbolic centrality of the Games, disinformation represented not just a reputational risk, but a potential trigger for unrest.

A third major pillar of the Paris 2024 threat environment lays in the existence of domestic dissents and civil disobedience. France has long been known for its intense activist nature, nonetheless we have seen in recent years a rise in spontaneous, decentralized, and sometimes violent protest. For example, the Gilets Jaunes movement between 2018 and 2020, as well as the nationwide pension reform strikes of 2023, demonstrated the capacity for large-scale mobilization to disrupt major infrastructures and overwhelming policing resources.[179]

The Olympics, as a global spectacle and symbol of state prestige, became a magnet for political protest. Although not inherently violent, movements leveraged the Games' visibility to advance anti-government, anti-elitist, or socio-economic grievances. Tactics included coordinated strikes, venue blockades, or flash-mob-style occupations, all of which posed challenges for security planners and raised the stakes for reputational management.

To mitigate these risks, the French government established "anti-disruption zones" and granted expanded powers to security services under Olympic-specific legislation. However, these

[178] European External Action Service, *Third EEAS Report on FIMI Threats*.
[179] Andreaa Voinea, Adrian Iacobini, and Teodora Dominteanu, "Paris 2024 Olympics: A Review of Innovation, Performance and Challenges," *Marathon – Journal of Economics and Administration* 16, no. 2 (2024): 153–62.

measures walked a fine line as it was the case in the context of London 2012 where excessive securitization became a source of contention and many saw it as an infringement to civil liberties.[180] Thus, the Host City Contract was created and signed to bound host nations to uphold fundamental rights alongside public order, requiring a delicate balancing act between deterrence and democratic legitimacy.[181]

Faced with this complex threat landscape, French authorities adopted a centralized, multi-agency strategy for security governance. The Préfecture de Police de Paris was given overarching responsibility for planning and coordination, working in collaboration with international bodies such as NATO, Europol, and Interpol.[182] Their training was done through scenario-based exercises, cyber-response drills, and intelligence-sharing mechanisms that were all scaled up in anticipation of multifaceted disruption.

AI and surveillance technologies

The 2024 Paris Olympic and Paralympic Games marked a pivotal moment in the evolution of public surveillance technologies in the organization of sports megaevents and in our case the Olympic and Paralympic Games. For the first time in French history, artificial intelligence-powered video surveillance systems were authorized for large-scale deployment in public space, under a legal framework designed specifically for the Games. This technological shift, driven by concerns over terrorism, crowd control, and public safety, was not merely operational; it signalled a broader transformation in how urban security is conceived, governed, and contested. As a result, Paris 2024 served as both a showcase for innovation as well as a laboratory for testing the legal and ethical limits of surveillance in an open society.

So, the legal framework that was created to assure that these AI and surveillance technologies would not provoke significant ethical issues was through the introduction of AVS. This tool was enabled by Law N°2023-380, adopted on the 19th of May 2023. This deployment of AI-powered

[180] Fussey, *Command, Control and Contestation*.
[181] CIO, *Contrat Ville Hôte – Principes.*
[182] Cour des comptes, *Rapport complémentaire au Parlement.*

video analytics in public spaces marked an unprecedented experiment in Olympic security governance. Validated by the Conseil d'État, one of the most important, Article 10, authorized the temporary deployment of automated video analysis systems to detect predefined anomalies in real time, such as crowd congestion, abandoned objects, sudden movement shifts, or individuals lying on the ground. Furthermore, the use of facial recognition and biometric identification was expressly prohibited, aiming to preserve alignment with the EU's GDPR (General Data Protection Regulation), and French privacy law. Article 10 permitted the use of AVS in both fixed and drone-based cameras, specifically for large-scale events involving significant public flows, thus adapting perfectly to an event such as the Olympic and Paralympic Games. It also included a sunset clause, a legal provision that automatically ends the law's effect unless renewed, authorization until the 31st of March 2025, and mandated data protection impact assessments before deployment. All algorithmic alerts had to be reviewed by human operators; this was done to prevent any possible automated enforcement errors.[183] Although the Conseil d'État upheld the constitutionality of Article 10, civil liberties groups raised concerns concerning transparency, oversight, and the risk of function creep. Many argued that even without biometric data, AVS could enable indirect profiling and set a precedent for embedding algorithmic surveillance into routine law enforcement. This was the case, for example, of La Quadrature du Net[184] and Amnesty International[185] that expressed concerns that the decision might set a legal precedent for normalizing mass surveillance under the guise of temporary experimentation.[186]

While AVS had no other precedent in French law for such a large-scale deployment in public space, it was made possible through a temporary derogation from France's strong privacy protections, notably the Data Protection Act as well as the EU's GDPR framework. The CNIL was assigned a dual oversight role: firstly, it reviewed the technical architecture of AVS systems and secondly it assessed their conformity to principles of necessity, proportionality, and transparency. Although, the CNIL issued guidance and conducted real-time evaluations, its

[183] République française, *Loi n° 2023-380*, 20 mai 2023.
[184] La Quadrature du Net, *Algorithmic Video Surveillance, Dangers and Counter-attacks*.
[185] Amnesty International France, *Pourquoi la vidéosurveillance algorithmique pose problème*.
[186] Alexandre Lodie and Stephanie Celis Juarez, "AI-Assisted Security at the Paris 2024 Olympic Games," HAL preprint (2023).

powers remained largely consultative, raising criticism from digital rights advocates who feared insufficient democratic safeguards.[187] [188]

Operational deployment centred on Cityvision, an AI surveillance platform developed by French start-up Wintics. According to Matthias Houllier, one of its co-founders, Wintics' system could detect a wide range of scenarios, from unattended baggage and suspected aggression to individuals sleeping in metro corridors or exhibiting erratic behaviour. Deployed in collaboration with the Ministry of the Interior, Préfecture de Police, SNCF as well as the French police, Cityvision operated through over 200 surveillance points across Paris, particularly in the metro, RER and Olympic transport corridors.[189] This platform's importance lays not only in its technical capabilities but also in its operational centrality. What I mean by this is that it served as the primary interface between AI-generated alerts and real-time decision-making. By enabling rapid human verification of algorithmic detections, Wintics played a pivotal role in ensuring that surveillance remained responsive, proportionate, and integrated into broader security protocols during one of the most complex public safety operations in French history.

Furthermore, Article 11 of Law No. 2023-380 expanded these powers, allowing for the real-time transmission of video streams to police command centres as well as the conditional storage of alerts for later analysis.

For these powers to be controlled, an evaluation committee, composed by the CNIL, the Conseil d'État, as well as parliamentary representatives, was created and given the powers to suspend any system that would violate legal thresholds for rights protection.[190] Despite this, critics raised concerns about the lack of public transparency, with algorithmic parameters often undisclosed and deployment zones not clearly marked.[191]

However, an element that further complicated the legal and democratic legitimacy of this experimentation was the risk of "function creep". Although designed as a temporary solution for an exceptional context, there were calls, such as those by Michel Barnier, French Prime Minister

[187] CNIL, *Observations de la CNIL sur le laissez-passer*.
[188] Zatsepina and Ludvigsen, *Algorithmic Olympics*.
[189] Wintics, *Cityvision*, 2024.
[190] République française, *Loi n° 2023-380*, 20 mai 2023.
[191] O'Brien, *Paris 2024 : French Government Approves Controversial AI Video Surveillance*.

at the time, for AVS integration into standard security policy.[192] Post-Games deployments during events like the Techno Parade and 2023 Rugby World Cup fan zones demonstrated the technology's lingering presence.[193] While some officials praised its ability to enhance crowd flow, the CNIL and civil society actors noted deceptive results and inconsistent weapon detection, showing the need for rigorous public debate on algorithmic surveillance's place in civic life.

As a result, Paris 2024 served as both an Olympic showcase of technological innovation and a critical test case for AI-enabled governance in democratic public space. Law No. 2023-380 played a central role in this experiment, illustrating how far the legal framework could be stretched when national security imperatives temporarily outweighed long-established privacy protections. The ongoing post-Olympic evaluations, both parliamentary and judicial, are now likely to influence the future trajectory of surveillance legislation not only in France but also in other liberal democracies grappling with the complex balance between technological advancement, public safety, and civil liberties.

Legal and policy reforms

During the preparations of such a megaevent that would host over 15 million visitors, 13 million ticketed spectators, and over 10,000 athletes during the Paris 2024 Olympic and Paralympic Games, the French government enacted an extensive package of legal reforms to ensure public safety at an unprecedented scale.[194] Among these legal reforms was the adoption of Law No. 2023-380, passed on 19 May 2023, introducing not only an operational innovation in Olympic security but as well as a significant legal and political inflection point in the governance of surveillance in France. While authorities saw the measures as a pragmatic response to potential terrorist threats, crowd management issues, and logistical complexity, civil society and digital rights organizations warned that it may signal a permanent erosion of civil

[192] Caddle, *AI Mass-Surveillance System*.
[193] *Marie de Vergès, Vidéosurveillance : attention à la dérive.*
[194] Cour des comptes, *Rapport complémentaire au Parlement.*

liberties under the guise of Olympic exceptionalism.[195] While the official justification from government officials was the anticipated complexity and risk of managing the Paris 2024 Olympic and Paralympic Games, this legal and policy reform quickly become the subject of debate in the entirety of the French society. Numerous questions were raised especially concerning the legal limits of surveillance in public space, the role of such exceptional measures in democratic societies such as ours and finally whether this so-called "temporary" experimentation would evolve into something more institutionally permanent.

The Olympic Games have long served as legal laboratories for exceptional security measures. Since the 1972 Olympic Munich Massacre, these mega events have been widely recognized as both targets of terrorism and catalysts for the expansion of state powers.[196] As a result, Law No. 2023-380 fits perfectly within this historical lineage. It was introduced specifically for the organization of Paris 2024 as it permitted, for the first time in French legal history, the experimental use of algorithmic video surveillance in public space, deploying software capable of detecting "anomalies" such as crowd density, abandoned items, or erratic human behaviour.[197]

Yet this law was not only about technological innovation but also a matter of statecraft and legal exceptionalism. By authorizing the suspension of France's otherwise strong data protection rules under a time-limited derogation, the state employed what is called a "securitization logic," in which constitutional constraints are temporarily relaxed in the name of public safety, something that would not be considered acceptable in most democracies.[198] This approach did not emerge in a legal vacuum. For this to be done correctly, France had already laid the legal groundwork for Olympic-specific adaptations through Law No. 2018-202 of 26 March 2018, which provided a foundational legal framework for hosting the 2024 Olympic and Paralympic Games. This law facilitated a range of exceptional provisions, including streamlined urban planning procedures, fast-tracked public procurement, and the reorganization of security and transport infrastructure specifically for the Games.[199] By enabling such derogations from ordinary administrative and environmental law, the 2018 statute institutionalized the idea that

[195] Nesser and Nasr, *The Threat Matrix Facing the Paris Olympics*.
[196] Blumenau, *Munich Massacre.*
[197] République française, *Loi n° 2023-380*, 20 mai 2023.
[198] Blumenau, *Munich Massacre.*
[199] République Francaise, *Law No. 2018-202 of 26 March 2018 on the Organisation of the Olympic and Paralympic Games of 2024*, Légifrance, 2018.

the Olympic Games required a parallel legal regime, this one being capable of overriding standard procedures in the name of efficiency, international visibility, and public order. As a result, such frameworks, in the context of post-2015 counterterrorism, reflect how states use crises, or in this case, mega-events, to recalibrate legal norms, not simply to address threats, but to reaffirm authority and sovereign control.[200]

Law No. 2023-380 incorporated a sunset clause, limiting the surveillance experimentation to the 31st of March 2025, therefore showing that the law had both functional and symbolic dimensions. Functionally, it was meant to secure a high-risk event. Symbolically, it was designed to reassure both citizens and international observers of France's control over urban risk. The government's narrative aligned itself with the framing used in London 2012, where Olympic security was presented as a performance of competence and modernity. In this context, legal reform became not only an act of governance but also a performative ritual of state legitimacy.

Furthermore, this law has implications for the broader legal system. This is due to the fact that even though facial recognition and biometric tracking were formally excluded, provisions upheld by the Conseil d'État, critics noted that algorithmic profiling could still occur. According to Amnesty International[201] and La Quadrature du Net,[202] such technologies risk creating a de facto "surveillance infrastructure" that can be adapted to other, more intrusive uses.[203]

Finally, an essential concern with this Law, No. 2023-380, is not only what it authorized during the Olympic period, but what it might enable after. What is meant by that is that already before the Games, AI surveillance tools were tested at public gatherings, such as the 2023 Rugby World Cup fan zones and the Techno Parade in Paris.[204] This operationalization of AVS outside of Olympic venues raises concerns of what legal scholars refer to as "function creep", the extension of exceptional legal measures into ordinary life.

In this context, these Olympic Games functioned as a policy incubator, allowing the French state to trial technologies in a socially and politically acceptable environment, under the protective justification of public safety. Many have warned that these legal tools developed for mega-

[200] Faucher and Boussaguet, *The Politics of Symbols*.
[201] Amnesty International France, *Pourquoi la vidéosurveillance algorithmique pose problème*.
[202] La Quadrature du Net, *Algorithmic Video Surveillance, Dangers and Counter-attacks*.
[203] Zatsepina and Ludvigsen, *Algorithmic Olympics*.
[204] *Marie de Vergès, Vidéosurveillance : attention à la dérive.*

events often “migrate” into permanent national policy after their immediate use expires.[205] The interest of figures such as Michel Barnier in embedding AVS in everyday policing frameworks illustrates this policy momentum.[206]

Law No. 2023-380 was surrounding by a governance structure that would include several oversight mechanisms such as the mandatory data protection impact assessments, the CNIL involvement and finally a special evaluation committee composed of members of the Conseil d’état, of the French Parliament as well as privacy regulators.[207] However, several legal experts and watchdogs have questioned the depth and independence of these controls.

Despite the fact that the CNIL played a consultative role and issued technical guidance, it had no direct power to halt deployments. This limited authority led many observers to conclude that algorithmic surveillance was rolled out with insufficient democratic safeguards, particularly in regard to transparency. Deployment zones were rarely clearly marked, and the detection logic of AVS systems remained classified, raising concerns about invisible governance.[208]

Ultimately, the importance of Law No. 2023-380 extends beyond Paris 2024. The legacy of Olympic security planning extends beyond physical infrastructure to include legal frameworks that often persist long after the Games have ended. France’s experiment with algorithmic surveillance fits this pattern: even if AVS is not formally made permanent, its large-scale deployment may reshape legal and institutional expectations about what forms of surveillance are acceptable in democratic urban spaces. In doing so, it risks normalizing exceptional security tools as part of everyday governance.[209]

This law now sits in a kind of legal grey zone, somewhere between the temporary and the permanent, between a one-time experiment and a lasting precedent. As the European Union moves toward establishing common rules on AI and biometric technologies, France’s Olympic surveillance experiment may well serve as either a cautionary tale or a policy model, depending on how it is evaluated and followed up in the months ahead.

---

[205] Jennings and Lodge, *Tools of Security Risk Management*.
[206] Caddle, *AI Mass-Surveillance System*.
[207] République française, *Loi n° 2023-380*, 20 mai 2023.
[208] Zatsepina and Ludvigsen, *Algorithmic Olympics*.
[209] Ramon Spaaij and Andrew Zammit, *The Terrorism Threat to the 2024 Paris Olympics: Learning from the Past to Understand the Present*, Short Read (The Hague: International Centre for Counter-Terrorism, June 27, 2024).

Although Law No. 2023-380 was introduced as a temporary response to the specific needs of the Paris 2024 Games, its impact could prove far more enduring. In practice, the law pushed the boundaries of France's surveillance laws, embedding AI tools into the very core of public safety operations during one of the most watched events in the world. This wasn't just a technical upgrade; it was a redefinition of what kinds of surveillance a democratic society is willing to tolerate. As lawmakers and courts begin reviewing the legacy of the Games in 2025, the real question is no longer just whether the law will expire as planned, but whether its effects will live on—quietly reshaping how public space is governed in the years to come.

Unique ceremony risks

The decision to host the Paris 2024 Olympic Opening Ceremony on the River Seine, a first in Olympic history, was widely praised as a bold expression of openness and cultural pride. Breaking with the traditional stadium model that has been done since the re-establishment of the modern Olympic Games in 1896 in Athens, it turned the entire city of Paris into a ceremonial stage, allowing the Games to speak from the heart of Paris and especially showcasing a big part of French culture.[210] The event featured a symbolic river parade, with music, lights, concerts and performances celebrating French heritage, from Simone Veil to Victor Hugo to Simone de Beauvoir, all of this visible to hundreds of thousands of spectators across the city. This open format promoted accessibility and national unity, including contributions from schoolchildren, regional artists, and overseas territories.[211] This opening ceremony also served a diplomatic purpose as it projected France as being resilient, progressive, inclusive, and culturally rich. This event was also a way of reinforcing national identity through rich storytelling especially in a period of social unrest where many members of the French population do not feel fully represented. Despite the numerous risks this ceremony presented, it showed its strength as a

[210] Paris 2024 Organising Committee, *Opening Ceremony of the Paris 2024 Olympic Games: Media Guide, 26-07-24, 19:30*, media guide, Paris 2024 Organising Committee for the Olympic and Paralympic Games, 2024.
[211] Préfecture de Police (Paris). *Security Arrangements for the Opening Ceremony of the 2024 Olympic Games*, press release, 2024.

tool to promote cultural diplomacy and collective representation.[212] Yet from a security perspective, it presented an unprecedented operational and strategic challenge. The Seine ceremony introduces a layer of logistical complexity not previously encountered in Olympic history, notably due to its lack of a confined perimeter, the multiplicity of entry and exit points, and the integration of public spaces such as bridges, docks, and streets into a live, urban performance space.[213]

At the heart of the concern was the exceptional exposure of both athletes and spectators to open urban environments. As indicated before, unlike traditional ceremonies held in enclosed, easily controlled stadiums, the 2024 Opening Ceremony took place across a vast stretch of central Paris, along the banks and bridges of the Seine. With over 300,000 people expected to attend, spread across ticketed and free-access zones, the potential for security breaches, overcrowding, and mass panic was quite high.[214] This decentralized layout significantly multiplied access points and escape routes, posing major challenges to perimeter security, crowd management, and emergency evacuation planning. The scale and openness of the event also created opportunities for both conventional and unconventional threats. Intelligence and counterterrorism agencies warned officials as well as Police officials the possibility of a broad spectrum of risks such as lone-actor attacks, vehicular ramming, coordinated mass shootings, and chemical or radiological threats.[215] Furthermore, the type of concern that was given a lot of importance were aerial threats, particularly drone incursions as they have become an important element in our current warfare. That is why this Opening Ceremony of the biggest and most important Sporting mega event on earth is a "prime target for airborne attacks", what is meant by this is that both contain the symbolic value of the event and the difficulty of securing vertical airspace in a dense urban setting. The possibility of swarming drones carrying explosives or surveillance payloads was deemed extremely likely, prompting authorities to install drone-jamming systems, anti-air radar, and low-altitude no-fly zones, coordinated by France's national aviation authority and military command structures.[216]

---

[212] Faucher and Boussaguet, *The Politics of Symbols*.
[213] Cour des comptes, *Rapport complémentaire au Parlement.*
[214] Préfecture de Police, *Security Arrangements for the Opening Ceremony*.
[215] Nesser and Nasr, *The Threat Matrix Facing the Paris Olympics*.
[216] Counterterrorism Group, "Threat Assessment Olympics Opening Ceremony Part 1: Airborne Attacks Very Likely; Strengthening of the Security Apparatus and Drone-Shield Systems Needed," July 1, 2024,

From a legal and institutional standpoint, the state's ability to manage such a dispersed event was bolstered by Law No. 2018-202, which laid the foundational legal groundwork for Olympic-specific adaptations, granting the state exceptional administrative powers to manage urban spaces and public order during the Games.[217] However, the practical challenge remained: how to ensure real-time situational awareness and crowd safety in an environment lacking conventional security enclosures?

From a legal and institutional standpoint, the French government ability to manage such a complex event supported by Law No. 2018-202. This legislation laid the foundational legal groundwork for Olympic-specific derogations and regulatory adaptations, granting French authorities' exceptional administrative powers to reshape urban planning, regulate public order, and facilitate rapid coordination across municipal and national bodies during the Olympic and Paralympic Games.[218] This law authorized the modification of traffic circulations plans, the creation of secure perimeter facilitating the movements of people and finally the temporary restriction of civil liberties in designated areas. All of these elements were essential in making this river-based ceremony a success for the athletes that would pass on their boats but as well as for the spectators that would be enjoying the event in the heart of the French capital. However, despite these numerous legal powers, this challenge remained quite formidable as there was a need to ensure real time situational awareness, risk mitigation and finally the protection of the crown in a fluid environment that lacked the physical barriers and entry controls typically associated with stadium security. The diffusion of spectators across bridges, embankments, and public spaces made it nearly impossible to establish a single secure perimeter. This required an important shift in security planning, moving from static defence to dynamic, surveillance and response systems. Operational command had to rely on a decentralised yet highly synchronised network of stakeholders, including the Préfecture de Police, Ministry of the Interior, Gendarmerie, fire brigades, transport operators, and private security actors, each who of course had their defined roles but linked through centralised coordination hubs.

To support this effort, a suite of digital tools and AI-powered technologies, notably the AVS systems enabled by Law No. 2023-380, were deployed to facilitate anomaly detection and rapid

[217] French Republic, *Law No. 2018-202*.
[218] French Republic, *Law No. 2018-202*.

alerting.[219] Nonetheless, the scale and novelty of the river-based ceremony pushed these systems to their operational limits. Because of this, there was a need for simulated drills, interoperability tests, and last-minute adjustments based on crowd modelling and weather conditions. In this context, legal preparedness and institutional adaptability proved essential, but were still contingent on real-time intelligence, inter-agency trust, and public cooperation to succeed under such unprecedented circumstances.

From an operational point of view, this deployment involved over 200 surveillance points, many equipped with Cityvision, an AI platform developed by French startup Wintics, which worked in close collaboration with the Ministry of the Interior, the Préfecture de Police, SNCF as well as French police forces.[220] These cameras, that were installed throughout metro corridors, along riverbanks, and in elevated areas, served as the digital backbone of the surveillance grid. Cityvision's algorithms enabled live detection of predefined anomalies, automatically flagging alerts to human operators who were responsible for verifying and escalating responses where necessary. This AI infrastructure was embedded within a broader security ecosystem that included anti-drone systems, airspace restrictions, boat patrols, physical checkpoints, and specialised incident response units. Facial recognition and biometric surveillance were explicitly prohibited, in keeping with GDPR and French data protection laws, but the AVS framework still raised ethical concerns about profiling, transparency, and post-Games normalization. Nonetheless, the AVS-driven model allowed for unprecedented responsiveness and situational precision, reflecting a shift toward predictive, data-centric urban security management during mega-events.[221]

Nevertheless, critics have warned that these innovations risk making the exceptional a normality whereby temporary surveillance powers established under the guise of public safety become fixtures of long-term urban governance.[222] The threat of 'function creep', where emergency measures are gradually absorbed into routine policing, looms large. This echoes certain analysis

[219] République française, *Loi n° 2023-380*, 20 mai 2023.
[220] Wintics, *Cityvision*, 2024.
[221] DGSI, *Plan Vigipirate*.
[222] Zatsepina and Ludvigsen, *Algorithmic Olympics*.

of post-crisis securitisation, in which security threats, that may be real or perceived, serve as catalysts for lasting legal and institutional shifts.[223]

So, the opening ceremony was not only used as a spectacle for cultural diplomacy but also as a symbolic and legal inflection point. This event was designed to "embody the spirit of openness and accessibility," yet its staging required an enormous security mobilisation unparalleled in French peacetime history.[224] More than 45,000 police, military, and private security agents were mobilised,[225] supported by real-time intelligence sharing across national and international agencies. The massive deployment and fusion of technologies, from drone jammers to cyber-defence shields, reflected a new Olympic security paradigm, where urban festivity and militarised vigilance coexist in uneasy balance.

To conclude, the openair Opening ceremony of the 2024 Paris Olympic and Paralympic Games have shown the dilemmas at the heart of megaevent security. It showed how it is possible to celebrate democracy and inclusiveness while mitigating the very vulnerabilities that such an event puts to the day. As a result, the legacy of this event, like that of London 2012 and Munich 1972, will lie less in its visual impact and more in its legal, technological and strategic precedents that it has laid for future democracies to organise safely these mega events.

C. Broader Contextual Framework

The Olympic Games are not just about sports and athletic performance; they are also moments when countries show the world who they are and who they want to be. Behind the events and medals, there is a powerful political, legal and cultural mix wiling to send a message around the world. Hosting the Games gives a country a chance to present itself as

[223] Blumenau, *Munich Massacre.*
[224] Paris 2024 Organising Committee, *Opening Ceremony Media Guide*.
[225] République française, *Plan A : ils l'ont fait !* Ministry of the Interior, published August 1, 2024; updated November 26, 2024.

strong, modern, and united, both to its own people and to the global audience watching. It is a way for nations to tell a story, not just about athletes, but about identity, ambition, and place in the world.

Since the 1972 Munich massacre, which saw the death 11 Israeli athletes and coaches killed by Palestinian Black September militants,[226] the magnitude of security of these mega-events has drastically change to the point where they now shape, and are shaped by, national policy, law, and international cooperation between various security services. During both London 2012 and Paris 2024, we have observed how hosting the Olympics can induce governments to treat these events as something far outside the ordinary. Scholars call this "event exceptionalism", this idea entails that mega-events are managed as extraordinary circumstances that justify temporary shifts or suspensions in normal legal, operational, and democratic procedures.[227] Security plans go beyond just keeping crowds safe; they often involve more police, more surveillance, and fewer opportunities for protest, all in the name of protecting the Games. These moments become a kind of stress test for democratic societies: therefore, it asks an important question for the entirety of society: how far can, or should, a government go to manage risk without compromising people's rights? [228]

Excluding for the tragic events of Munich 1972, the risk of terrorism has not disappeared since then and it was the case during the 1996 Atlanta Games, when a bomb detonated in Centennial Olympic Park, killing two people and injuring over 100. The attack, conducted by Eric Rudolph, later identified as a domestic terrorist motivated by anti-government and anti-abortion beliefs, exposed critical weaknesses in the United States' approach to event security. Despite heightened vigilance following the 1995 Oklahoma City bombing, the reliance on traditional perimeter-based security proved insufficient in detecting and preventing threats that emerged from within. According to the FBI, Eric Rudolph evaded capture for five years, underscoring both the complexity of domestic terrorism and the limits of conventional security responses.[229] In the aftermath, the U.S. began to rethink its Olympic security strategies, shifting toward integrated

[226] Blumenau, *Munich Massacre.*
[227] Fussey, *Command, Control and Contestation*.
[228] Zatsepina and Ludvigsen, *Algorithmic Olympics*.
[229] Federal Bureau of Investigation, *Eric Rudolph*, FBI History: Famous Cases, n.d.

surveillance systems and improved inter-agency coordination, particularly between federal bodies like the FBI, FEMA, and newly evolving homeland security structures.[230]

This evolving logic of "special event security" became even more pronounced later on during another Games. The 2004 Athens Olympics, unfolded in the shadow of the 9/11 attacks on the World Trade Centre, therefore starting the global "war on terror," and ongoing instability in Iraq and more generally the entirety of the Middle East. As a result, Greece mounted what was then the most expensive Olympic security operation in history, exceeding $1.5 billion. This immense budget was put to good use with the hiring and deployment of over 70,000 personnel, NATO aircraft and AWACS patrolled Greek skies, and, for the first time in peacetime, a non-wartime EU member state installed U.S.-made Patriot missiles as a precautionary measure.[231] [232] This unprecedented militarization of public space signalled a new norm: hosting the Olympics now required not only financial and infrastructural investment, but also a full-scale security architecture comparable to counterterrorism operations.

By the 2008 Beijing Games, the security paradigm had further evolved, however this time it was shaped as much by political control as by external threat. China's strategy extended well beyond the prevention of terrorist acts, encompassing the suppression of political dissent and the widespread surveillance of ethnic and religious minorities, notably in Tibet and Xinjiang. As Human Rights Watch reported, the Chinese government used the Olympics as a justification to intensify crackdowns, detain activists, and censor dissenting voices, all in the name of national stability and global image management, especially in a way to show the capacity of the Chinese government to control its population and organize the best possible Olympics.[233] These actions triggered international criticism and raised fundamental questions about the ethical costs of hosting the Games in authoritarian contexts, where "security" can serve as a blanket term for repression.

---

[230] Christopher Bellavita, "Changing Homeland Security: A Strategic Logic of Special Event Security," *Homeland Security Affairs* 3, no. 3 (2007).
[231] Voice of America, "Unprecedented Security Measures in Place Ahead of Olympics Opening Ceremony," *VOA News*, August 12, 2004.
[232] Jason J. Brianas, *NATO, Greece and the 2004 Summer Olympics*, thesis, Naval Postgraduate School, 2004.
[233] Human Rights Watch. "China: Crackdown Violates Olympic Promises," *Human Rights Watch*, February 6, 2008.

Taken together, these cases illustrate how Olympic security has become a flexible and adaptive tool, shaped by domestic political contexts, global fears, and the strategic demands of visibility. From Atlanta to Athens to Beijing, to London and finally last year to Paris, the Olympics have not only reflected the evolving nature of global threats but have also revealed how host states define, and often stretch, the boundaries of legitimate state power in moments of international scrutiny.

Both London and Paris have operated under the long and evolving shadow of the post 9/11 security paradigm, an era in which terrorism ceased to be seen as a distant, isolated threat and instead became understood as a diffuse, hybrid, and enduring risk embedded within everyday life. The securitization of international sporting mega events intensified dramatically after the attacks on New York and Washington in 2001 and was further reinforced by subsequent bombings in 2004 in Madrid and in 2005 London. Each of these incidents amplified the understanding that high-profile, mass-attendance events, like the Olympic Games, are not just logistical and symbolic feats, but also prime targets for groups seeking global attention and political impact.[234] [235] The sheer concentration of people, media, and national pride at the Olympics transforms them into ideal stages for both celebration and disruption.

In response, host states have increasingly embraced anticipatory security logics: this means implementing a strategic mindset where security planning is not only based on known or credible threats, but also on imagined, speculative, or probabilistic risks.[236] This shift enables governments to justify exceptional measures, such as expansive surveillance, legal exceptions, or militarized policing, on the grounds of pre-emption. In this model, the mere possibility of a threat can gives the possibility to the government to do intrusive or enduring interventions, creating a security environment shaped as much by fear and foresight as by evidence.

In the United Kingdom, the bombings that took place the 7th of July 2005 had a profound and lasting influence on the security architecture that would later shape the London 2012 Olympic Games. Occurring just a day after London was awarded the Games, the attacks placed the forthcoming event in the direct trajectory of a national counter-terrorism overhaul. The UK's

[234] Crilley, *Urban Militarisation and the 2012 London Olympics*.
[235] Spaaij and Zammit, *Terrorism Threat to the 2024 Paris Olympics*.
[236] Louise Amoore, "Algorithmic War: Everyday Geographies of the War on Terror," *Antipode* 41, no. 1 (2009): 49–69.

response emphasized fusion across intelligence and law enforcement agencies, behavioural surveillance in public spaces, and a broader pivot toward intelligence-led policing.[237] [238] Central to this approach was the CONTEST strategy, built on four pillars: Pursue, Prevent, Protect, and Prepare. While "Pursue" focused on identifying and disrupting plots, "Prevent" aimed to counter radicalization at the community level, blending traditional law enforcement with soft power tools such as education, outreach, and local partnerships.[239] Olympic security thus became a proving ground for this integrated model, testing not just coordination, but also public acceptance of heightened surveillance and behavioural profiling in everyday spaces.

France followed a parallel but more legally radical path. The wave of attacks in Paris and Nice between 2015 and 2016, including the coordinated assaults on the Bataclan and Stade de France, pushed the French state and government to adopt a posture of permanent vigilance. Emergency powers initially granted under temporary provisions were gradually folded into ordinary law, marking a significant shift in the balance between civil liberties and state authority. Legislative changes and constitutional amendments expanded police powers, redefined thresholds for detention and search, and gave legal cover to expansive surveillance programs. By the time Paris was preparing to host the 2024 Games, this security posture had become institutionalized. Framed as a pragmatic response to enduring threats, it enabled the rollout of controversial technologies, including algorithmic video surveillance and AI-assisted behaviour recognition, under the exceptional banner of Olympic necessity.[240] What was once seen as extraordinary had, in effect, become routine.

Taken together, the experiences of London and Paris illustrate how the Olympic Games, in the post 9/11 era, have become laboratories for new forms of security governance. They reveal not only how democratic states respond to terror, but also how they redefine the boundaries of what is legally, ethically, and politically acceptable in the name of national safety and international prestige.

These legal experimentations, which were considered as temporary, exceptional, or strictly time-bound, rarely vanish once the Games end. Instead, they often create precedents for lasting

[237] United Kingdom, *London 2012 Olympic and Paralympic Safety and Security Strategy*, March 2011.
[238] Committee of Public Accounts, *Post-Games review.*
[239] Jennings and Lodge, *Tools of Security Risk Management*.
[240] République française, *Loi n° 2023-380*, 20 mai 2023.

shifts in governance. The regulatory experiments piloted under Olympic urgency tend to seep into ordinary legal frameworks, a phenomenon certain scholars refer to as "policy creep" or "normalization through exception".[241] For instance, the extensive surveillance infrastructure and security protocols introduced for 2012 London Olympic and Paralympic Games were later integrated into broader policing and counterterrorism strategies, particularly in urban areas considered as "high-risk." In France, although the AI surveillance powers were allegedly restricted to the Olympic period, advocacy groups have warned and indicated that the technological ecosystem and institutional momentum behind them are unlikely to disappear quietly once the Games end.

Therefore, what has emerged is a troubling pattern: the logic of exception has become a pathway to permanence. Laws and technologies justified by the unique demands of mega-events often bypass regular democratic scrutiny, shielded by the rhetoric of urgency, security, and national pride. This dynamic is not limited to surveillance. It extends to obtaining fast-tracking, public protest restrictions, forced relocations, and the commercialization of public space, each framed as necessary sacrifices for the success of a "once-in-a-lifetime" occasion.

Moreover, the legal elasticity granted to host states during the Olympic window reflects a deeper shift in how urban security is imagined and governed. Instead of reacting to threats, cities, such as London and Paris, are increasingly reconstructed to anticipate and prevent them, meaning pre-crime logics that recast entire populations as potential risks to be monitored, modelled, and managed. In this predictive security paradigm, law becomes less about rights and due process and more about data, algorithmic probabilities, and strategic containment.

Importantly, this evolving legal architecture is not merely technical, it is profoundly political. The choices made about what to regulate, whom to monitor, and which technologies to deploy reflect broader questions about who belongs in public space, whose security matters, and how power is exercised in the name of safety. The Olympic Games thus function not only as a showcase of athletic prowess and national image, but as high-stakes testing grounds for future-facing forms of techno-legal governance. What begins as the Olympic necessity often becomes democratic legacy, raising urgent questions about transparency, accountability, and the price societies are willing to pay for spectacle.

[241] Boyle and Haggerty, *Planning for the Worst*.

The Olympic Games are not only athletic competitions, but they are also arenas with a powerful symbol in which states perform their identity, competence, and legitimacy for both domestic and international audiences. In this context, security planning becomes performative, not simply about preventing threats, but about projecting authority, technological capability, and finally care for the well-being of the public. The staging of security thus communicates more than safety; it conveys a vision of the state itself. This was particularly evident with the decision to hold the Paris 2024 Opening Ceremony on the Seine, a bold logistical and political move that transformed the traditional stadium format into an open-air spectacle. The choice was deliberate as it signalled cultural openness, civic accessibility, and technological sophistication, all underpinned by an enormous and mostly invisible security apparatus.[242]

Similarly, London 2012's security discourse revolved around the language of proportionality and reassurance. Officials described a "layered" system that combined high-visibility deterrents, such as surface-to-air missile placements and armed patrols, with nonvisible elements like intelligence operations, behavioural detection, and community-based initiatives. The goal was to calm public fears without evoking a state of siege.[243] In both cases, the security strategies were as much about public messaging as they were also about operational effectiveness. Through their choices, planners aimed to balance strength with subtlety, projecting control while preserving the festive, inclusive spirit of the Games.

However, this performative dimension of security does have a few contradictions. When protective measures become too visible, military vehicles on city streets, ubiquitous surveillance cameras, or bag checks at every turn, this may evoke fear rather than confidence. This paradox, often described as "spectacular security" is the idea that the visual and theatrical display of safety measures can actually undermine the sense of safety they are meant to reinforce.[244] In attempting to visibly demonstrate control, the state risks amplifying public anxieties and drawing attention to potential vulnerabilities.

Both London 2012 and Paris 2024 have navigated and gone through this tension quite carefully. Too little visibility could be perceived as a weakness, and too much might alienate the public or provoke criticism concerning the militarization of civic space. Furthermore, these high-profile

[242] Paris 2024 Organising Committee, *Opening Ceremony Media Guide*.
[243] George and Mawby, *Security at the 2012 London Olympics*.
[244] Fussey, *Command, Control and Contestation*.

displays often generate wider debates about civil liberties, the right to privacy, and the future of public space. Critics of these Olympic Games raised concerns about the normalization of surveillance technologies, the presence of armed forces in urban environments, and the potential long-term legacy of security measures introduced under the exceptional logic of mega-events.

In this way, the securitization of the Olympics becomes offers a dual performance: on the one hand it is aimed to deter adversaries and reassure citizens, and on the other hand it inadvertently reveals the limits and consequences of governing through spectacle. As the boundaries between public celebration and security theatre are blurred, Olympic hosts must reckon not only with logistical challenges, but with profound questions about the kind of society they wish to project, preserve, in the process.

One of the most persistent concerns in the aftermath of Olympic security planning is the risk that temporary, exceptional powers become permanent features of governance. While emergency measures are often justified in the context of mega-events as time-limited and proportionate, history shows that once such powers are introduced, particularly when they involve innovative technologies, institutional restructuring, or significant financial investment, they are rarely rolled back in full. In effect, the state of exception becomes routinised, woven into the fabric of everyday law enforcement and public administration.

This dynamic was evident in the legacy of London 2012, where elements of the Olympic security infrastructure were quietly adapted for broader domestic counter-terrorism efforts. Surveillance platforms initially introduced to protect Olympic venues, as well as inter-agency coordination models piloted during the Games, became integrated into the UK's broader security ecosystem.[245] What was once framed as extraordinary became the new normal, often without renewed public debate or formal legislative scrutiny.

In France, the early rollout of AVS at pre-Games events, such as Rugby World Cup fan zones as well as the Techno Parade, signalled a similar process of function creep, where technologies introduced under the guise of Olympic necessity begun to migrate into everyday policing.[246] Though facial recognition remains legally prohibited, AVS systems rely on behavioural analytics

[245] Paul Burnham, *Multi-Agency Interoperability at Major Sporting and Sailing Events* (Doha: Josoor Institute, January 2021).
[246] Zatsepina and Ludvigsen, *Algorithmic Olympics*.

and anomaly detection, which raise equally profound questions about profiling, consent, and algorithmic opacity. As these systems become embedded in local law enforcement practices, the temporary boundary between event security and routine surveillance grows increasingly blurred.

The stakes of this transition extend beyond national borders. With the European Union actively developing regulatory frameworks for artificial intelligence, biometric surveillance, and data protection, through instruments such as the AI Act, GDPR, and initiatives from the EEAS, France's experiment with Olympic surveillance could shape legal precedents at the continental level. If the Paris 2024 security model is widely seen as a success, measured in terms of incident prevention, crowd control, and international prestige, then Law No. 2023-380 may be cited as a policy template for future mega-events and urban security governance. Conversely, if the Games are perceived as overly securitized, opaque, or disrespectful of civil liberties, they may serve as a cautionary tale, a moment when democratic societies realize the cost of confusing visibility with legitimacy, and safety with compliance.

Finally, Paris 2024 marks a legal and institutional crossroads. It offers an opportunity to interrogate how liberal democracies manage risk under pressure, and whether temporary measures justified in moments of exception can truly remain exceptional. The challenge lies not just in protecting spectators and athletes, but in protecting the democratic norms and legal safeguards that mega-events so often put to the test. In this sense, the Olympics become a mirror, not just of national identity, but of how far societies are willing to go, and what they are willing to sacrifice, in the name of security.

The Olympic Games are more than about medals and flags. They are about who we are as nations, how we present ourselves to the world, and how we protect what matters most. London 2012 and Paris 2024 show us that when a city hosts the Olympics, it also becomes a stage for something else: how governments handle fear, power, and public trust under the global spotlight.

In London, the memory of the 2005 bombings shaped a careful, layered approach to security, focused on intelligence, cooperation, and being visible but not overwhelming. In Paris, shaped by the pain of 2015, the government turned to innovative technology: cameras that detect "abnormal" behaviour, drones, and real-time data analysis. Both cities tried to keep people safe

but also faced tough questions about what that safety costs in terms of privacy, rights, and democratic life.

Because the truth is, it is not just about what governments can do, it is about what they should do, and whether people feel that the trade-offs are fair. You cannot force public trust; it has to be earned, and it can easily be lost when security feels more like control than protection.

As we look toward future Olympics, from Los Angeles to Brisbane and who knows where, the big question does not go away: How do we protect these shared moments without losing the values they are meant to celebrate? Finding that balance between safety and freedom, between innovation and oversight, is not just a challenge for host cities. It is a test of the kind of society we want to be.

Part III – Comparative Analysis

Throughout this part, I will compare how London 2012 and Paris 2024 approached Olympic security, focusing on how threats were framed, how technology and law were mobilized, how governance and coordination were managed, and how the public and media perceived these choices, in order to show both national differences and shared lessons.

A. Threat framing

Security planning for the Olympic Games has never been and will never be neutral. Being global mega-events, means that the Summer Olympics attract not only attention but symbolic, political, and tactical risks. In this context, it is essential to examine how authorities threat framing plays a decisive role in shaping security strategies. As a result, this section examines and compares how the United Kingdom and France, leading up to London 2012 and Paris 2024, have constructed threat narratives. Drawing on official government documents, counter-terrorism strategies, and academic studies, it shows how each state interprets Olympic vulnerability through its own political culture, institutional memory, and operational doctrine. The aim is to assess how different logics of threats have justified legal exceptionalism, informed technological choices, and altered the Olympic experience itself.

The Role of Historical Trauma in Framing Olympic Risk

Olympic security doctrine has long been shaped by past tragedy. In 1972, the Munich attacks, during the Olympic Games, perpetrated by members of the terrorist organization Black September on athletes of the Israeli delegation attack marked a global turning point, compelling states to shift from reactive to preventive security planning. Munich's legacy established the Olympics as a permanent high-risk period, especially vulnerable to

politically motivated violence. This historical rupture gave rise to a new global discourse of Olympic vulnerability, one which has been absorbed into national security logics ever since.[247]

In the case of London 2012, trauma was not only inherited from Munich but also from domestic events. The 7th of July 2005, the London Bombing, which occurred just one day after the announcement that London had secured the Olympic bid, intensified national security anxieties and catalysed an immediate policy shift. Those attacks, perpetrated by British citizens inspired by transnational jihadist ideologies, highlighted the danger of homegrown terrorism and exposed coordination failures within the UK's intelligence architecture. The Intelligence and Security Committee's post-attack report insisted on the need for a fix in threat detection, inter-agency communication, and urban preparedness.[248] The British Transport Police archives indicate that the symbolism of both the location, the London Underground, and the timing, post-Olympic bid, were seared into the national consciousness as indicators of systemic vulnerability.[249]

This tragic event became foundational during the framing of the 2012 Games, not only as a sporting celebration but as a potential repetition for mass violence. The government's response materialized in a deepened and revised CONTEST strategy, emphasizing pre-emption, radicalization prevention, and community surveillance. In short, the 7/7 bombings legitimized a turn toward systemic counterterrorism embedded in everyday policing and national discourse.[250]

In France, however, this traumatic narrative is even more recent and has, unfortunately, continued to take place. The succession of major attacks between 2015 and 2020, beginning with the Charlie Hebdo and Hyper Cacher assaults, peaking with the Bataclan massacre, and extending to the truck attack in Nice and the killing of schoolteacher Samuel Paty, has saturated the French security landscape with a sense of enduring, diffuse danger. These events were not isolated shocks but layered wounds. The state's use of these attacks to justify constitutional exceptionalism has led to the permanent entrenchment of measures once deemed temporary.

[247] Blumenau, *Munich Massacre.*
[248] UK Government, *Response to ISC Report on 7 July 2005 Attacks.*
[249] UK Government, *Government Response to the ISC Report* (2006).
[250] Home Office (UK), *London 2012 Olympic and Paralympic Safety and Security Strategy.* London (2009).

States of emergency became a routine, meaning the expansion of police powers and intelligence surveillance became default.[251]

The Ministry of the Interior, through its flagship intelligence agency DGSI, has since crafted a narrative wherein the Olympic Games are not merely "at risk" but emblematic of France's national strength and ideological vulnerability. The *Security in the Name of Festivity* publication illustrates this logic: Olympic security is no longer about technical prevention alone but a choreographed affirmation of the Republic's protective capacity. The Games are framed as a stage where resilience must be visibly performed.[252]

What emerges in both contexts is the instrumental use of trauma, not only to drive reform, but to reframe the role of the state. In the United Kingdom, trauma prompted structural recalibration and in France, it ushered in legal exceptionalism and public rituals of securitization. Trauma, then, is both a policy catalyst and a narrative device. It allows security planners to reframe extraordinary legal and technological measures as logical extensions of national self-defence. Crucially, however, the emotional and temporal distances differ. While the UK has institutionalized its trauma, France is still in the act of commemorating it, blending grief with policy in ways that make democratic contestation more difficult.

National Security Doctrines: CONTEST vs Plan Vigipirate

The construction of a threat is not merely discursive; it is embedded within the institutional architecture. In both the UK and France, the operationalization of an Olympic threat framing occurs through codified national counter-terrorism strategies, in the United Kingdom it is known as CONTEST and in France it is known as Plan Vigipirate. These frameworks do more than guide policy, they define how risk is understood, who holds authority, and what level of democratic scrutiny is permissible during mega-events.

[251] Faucher and Boussaguet, *The Politics of Symbols*.
[252] The Olympic and Paralympic Games: Security in the Name of Festivity, *Direction Générale de la Sécurité Intérieure (DGSI)*, published November 28, 2023; updated November 26, 2024.

The UK's CONTEST strategy was first articulated in 2003 and substantially revised in 2009 and 2011. It is built on four pillars: Pursue, Prevent, Protect, and Prepare. Each of them represents a domain of state action, from disrupting terrorist networks to reinforcing infrastructure to fostering community resilience. The strategy's holistic nature has reflected a post-7/7 consensus: that effective counterterrorism demands integration across intelligence, policing, and civil society.

The government's reply to the Home Affairs Committee's 2008–09 report on CONTEST[253] reveals the strategic adaptations made in the lead-up to London 2012. Among those strategic adaptations there was an increased emphasis on lone actor threats and self-radicalized individuals, a response directly shaped by the 2005 bombings. Intelligence coordination was strengthened through JTAC, and local policing was linked to national security via Prevent and Channel programs.

This comprehensive approach informed the Olympic Safety and Security Strategy, which explicitly described the Games as a "threat-led, intelligence-driven" undertaking. The integration of MI5 threat assessments with OSSSRA framework enabled the dynamic prioritization of threats based on both likelihood and impact. Importantly, the UK's model favoured layered defence, not just high-visibility patrols or physical barriers, but fusion centres, intelligence sharing, and what might be termed *soft surveillance* meaning mechanisms embedded in routine governance rather than visible spectacle.[254]

France's equivalent framework, Plan Vigipirate, has a longer lineage but has undergone fundamental transformation since the 2015 wave of terrorist attacks. Originally adopted in 1978 to manage Cold War-era threats, Vigipirate was historically focused on visible deterrence: military patrols in train stations, security alerts in public buildings. However, its post-2015 iteration is radically different, reflecting a transition from static defence to adaptive, high-alert governance.

The revised version, formalized in 2016 and refined in subsequent years, divides risk into three "vigilance levels," each triggering progressively expansive measures, from bag checks to

[253] Home Office (UK), *London 2012 Olympic and Paralympic Safety and Security Strategy.* London (2009).
[254] United Kingdom, *London 2012 Olympic and Paralympic Safety and Security Strategy*, March 2011.

curfews, and from expanded border controls to intelligence-based interventions.[255] Unlike CONTEST, which functions within a decentralized governance model, the Plan Vigipirate is centralized, executive-driven, and anchored in France's internal security doctrine, notably through the Ministry of the Interior and its direct oversight of the DGSI.

For Paris 2024, the Games have been identified as subject to the "scarlet" alert level, the highest in the framework. This level presumes constant threat and grants the state maximal discretion in applying restrictive measures. Operational command is unified under the Ministry of the Interior, integrating police forces, military patrols (notably Operation Sentinelle), intelligence agencies, and more and more private actors tasked with technological implementation.[256] This logic here is one of concentration: risk is seen as systemic, and therefore, the state response must be centralized, totalizing, and rapid.

This divergence between these two models is not merely technical, it reflects distinct political cultures and legal traditions. The UK's approach relies on existing legislative frameworks, and is shaped by an adversarial parliamentary culture, and is constrained by norms of proportionality and judicial review. France's model, in contrast, is shaped by executive power, securitized republicanism, and the enduring legacy of the état d'urgence. This distinction is seen clearer in their handling of exceptional powers. On the one hand, the UK's security expansions post-7/7 were often framed as temporary and corrective and on the other hand France's post-2015 measures, many of which now underpin Olympic preparations, have been increasingly codified into ordinary law.

Furthermore, the framing of threats within these strategies differs in scale and abstraction. CONTEST is structured around the notion of *resilience* meaning the management of threats through distributed risk governance, societal buy-in, and procedural safeguards. Vigipirate is built around *fortress logic* meaning that the state is seen as a bulwark, protecting the national body against incursion, contamination, or collapse. This logic has important consequences: in the UK, community engagement is part of the counter-terror toolkit and in France, it is often subordinated to centralized risk calculus and symbolic displays of force.

[255] DGSI, *Le Plan Vigipirate*.
[256] Cour des comptes, *Rapport complémentaire au Parlement.*

So, in summary, while both CONTEST and Vigipirate function as blueprints for Olympic security, they do so through fundamentally different institutional logics. The United Kingdom's model is multi-agency, intelligence-centric, and strategically invisible. France's is hierarchical, legally exceptional, and deliberately visible, with state authority projected as spectacle. These models reflect not just divergent threat assessments, but deeper divergences in how each democracy reconciles security imperatives with governance norms.

From OSSSRA to Algorithmic Surveillance: Operationalizing Threat

A key difference in how London 2012 and Paris 2024 have framed and acted upon threats has lied in the tools and epistemologies they have used to assess and govern risk. In London, OSSSRA served as the backbone of strategic planning. Developed in collaboration with MI5, local police units, and national infrastructure bodies, OSSSRA was a structured analytical framework designed to rank, calibrate, and prioritize threats based on traditional probabilistic models. Its methodology reflected an engineering-inspired logic of risk: measuring threats in terms of likelihood and impact and distributing resources accordingly.[257]

Furthermore, the OSSSRA model massively relied on human intelligence and known threat profiles. Although enhanced by technological tools such as CCTV and ANPR (Automatic Number Plate Recognition), the system was grounded in established laws and did not push legal or ethical boundaries. Surveillance was extensive but legally conventional and justified as a means of amplifying coordination rather than experimenting with new forms of population management. This aligned with the UK's broader preference for "embedded security", integrating counter-terror practices into existing urban and legal infrastructure without overt disruption to daily life.[258]

On the other hand, Paris 2024 represents a radical departure from this model. Instead of relying solely on risk models or conventional surveillance, the French state has embraced an algorithmic model of threat detection. The passage of Law No. 2023-380 marked a decisive moment in the

[257] United Kingdom, *London 2012 Olympic and Paralympic Safety and Security Strategy*, March 2011.
[258] United Kingdom, *Project CONTEST.*

legal architecture of public security, authorizing, for the first time in French history, the deployment of AI-enhanced video surveillance in public space for a national event. The law allows for real-time analysis of video feeds by software capable of identifying behavioural anomalies, object abandonment, unauthorized incursions, and crowd movement irregularities.[259]

An important element that distinguishes this legal innovation is not only its technological ambition but its discursive framing. The law's preamble refers to an "unprecedented convergence of threats, meaning a justification that blends the jihadist legacy of recent years with the newer, more diffuse risks posed by cyberattacks, drone incursions, far-right violence, and social unrest. Many critics have appeared, from civil liberties organizations to CNIL, warning that such experimentation risks creating a precedent for permanent algorithmic governance of public space and could endanger the life of the French population. [260]

Some concerns have been raised surrounding the implementation asymmetries, data governance, and accountability gaps. It has been seen in a report from the French Cour des Comptes that there is a logistical fragmentation between contractors, blurred lines of responsibility, and insufficient oversight mechanisms, especially regarding data retention, algorithmic bias, and interoperability with existing police systems.[261] These operational concerns are compounded by the DGSI's internal ambition, stated in its 2023 report *Security in the Name of Festivity*, to transition from a "reactive" to a "predictive" paradigm of urban security.[262]

In other words, France is not merely responding to known risks but rather attempting to anticipate and pre-empt emergent disruptions before they materialize. This represents a fundamental epistemological shift: from understanding risk as a calculable future event to treating it as a latent presence, constantly monitored and governed through digital proxies.

By contrast, London's approach to surveillance and risk detection in 2012 was institutionally cautious and legally conservative. The UK did not introduce any bespoke legislation to expand surveillance powers for the Games. Instead, it relied on the existing surveillance apparatus, CCTV coverage, border watchlists, and targeted policing, augmented through inter-agency

[259] République française, *Loi n° 2023-380*, 20 mai 2023.
[260] CNIL, *Observations de la CNIL sur le laissez-passer*.
[261] Cour des comptes, *Rapport complémentaire au Parlement.*
[262] DGSI, *Security in the Name of Festivity*.

collaboration rather than technological reinvention.[263] This reflects the UK's constitutional preference for discreet normalization: enhancing control through soft law and administrative routines rather than headline-grabbing legal changes.

Thus, the divergence between OSSSRA and France's algorithmic system is not simply a matter of technological advancement, but rather of governance philosophy. On the one hand, London 2012 framed surveillance as a logistical tool, supporting layered defence within existing norms. On the other hand, Paris 2024 frames it as a norm-shifting experiment, where AI becomes both a security instrument and a legal precedent. In doing so, France positioned Olympic security as a laboratory for new governance models, with potential implications far beyond the Games.

Hybrid Threats and Informational Warfare

One of the most significant evolutions between London 2012 and Paris 2024 is the shift from mono-causal to hybrid threat framings. London 2012, while sensitive to a broad range of risks, was primarily constructed around the threat of jihadist terrorism and the challenge of domestic radicalization. Its security strategy was designed with a relatively clear adversary in mind, and counter-terrorism measures were rooted in intelligence work, physical protection, and public reassurance. By contrast, Paris 2024 emerges within a more diffuse, networked, and hybridized threat environment, including cyberattacks, drone incursions, disinformation campaigns, and far right and far left extremism.[264]

This hybridization is not merely an analytical update, but it has profound implications for how the Olympic Games are governed. Whereas traditional threat matrices relied on probability and precedent, the new environment requires states to govern uncertainty. Hybrid threats blend physically and digitally, the kinetic and the symbolic. A single drone, a falsified video, or a coordinated disinformation campaign can now disrupt Olympic operations, erode public trust, or provoke disorder, all without the use of any type of physical violence.

[263] United Kingdom, *London 2012 Olympic and Paralympic Safety and Security Strategy*, March 2011.
[264] Nesser and Nasr, *The Threat Matrix Facing the Paris Olympics*.

The EEAS has warned that foreign information manipulation and interference (FIMI) pose an escalating threat to democratic resilience, especially during globally visible events like the Olympics. Russia, in particular, has been identified as a key player in shaping narratives that seek to delegitimize France's capacity to organize the Games, often through AI-enhanced propaganda disseminated via social media and fringe news outlets. These information operations exploit existing grievances, spread conspiracy theories, and sow distrust in the state's ability to secure both physical and cognitive space.[265]

This shift has triggered a strategic reframing of Olympic security: no longer confined to protecting physical infrastructure, it now encompasses the defence of public perception and national legitimacy. For Paris 2024, this means surveillance systems are designed not only to detect bombs or unauthorized access, but to identify "anomalous discourse, including hate speech, online mobilization, or the viral spread of falsehoods that could incite panic or violence.

While London 2012 acknowledged cyber risk, it treated it as a technical challenge, largely confined to infrastructure protection. This means, for example, the prevention of network failure, ticketing disruption, or communications breaches. Disinformation and perception warfare were not central concerns in its security doctrine. By contrast, Paris integrates these concerns at the highest levels of planning. The DGSI, in its 2023 strategic guidance, outlines an "informational theatre of operations" to be monitored alongside the physical one.[266]

This evolution reflects a broader epistemic shift in threat management: from policing bodies to policing narratives. In this sense, Paris 2024 illustrates the convergence between national security and information control. This is a trend that raises new questions about freedom of expression, data governance, and the future of democratic discourse in the age of algorithmic surveillance.

Democracy, Legitimacy, and the Performativity of Threat

[265] European External Action Service, *Third EEAS Report on FIMI Threats*.
[266] DGSI, *Security in the Name of Festivity*.

While both London and Paris framed Olympic threats as requiring strong state responses, the democratic implications of these framings diverge significantly in their scope and structure. In the UK, the CONTEST framework, although extensive, remained largely embedded within pre-existing legal architecture. It was subject to parliamentary scrutiny, judicial oversight, and public debate. Measures such as Prevent were controversial, but they unfolded within a normative framework that presupposed eventual rollback or review. The legal ethos was one of temporary proportionality: extraordinary measures were justified by extraordinary circumstances, but with institutional pathways for return to normalcy.[267] [268]

On the other hand, France has increasingly exhibited what scholars refer to as legal "permanentisation" meaning exceptional powers granted for temporary security crises become woven into the permanent fabric of law. Law No. 2023-380, which authorizes algorithmic surveillance during the Olympic period, is emblematic of this drift. Ostensibly experimental and time-bound, it opens the door to future extensions and normalization.[269] France's post-2015 trajectory reveals a form of "experimental authoritarianism", a governance model where innovation in security policy often bypasses conventional democratic safeguards in the name of agility and responsiveness.[270]

Moreover, the French approach is overtly performative. The Olympic Games are not merely an object of protection, but a theatre in which state power is staged and celebrated. The visible deployment of troops, surveillance infrastructure, and algorithmic control is designed not only for functionality but for spectacle. The absence of a terrorist attack becomes a narrative of success, not just for security professionals, but for the state itself. As such, the Olympic security plan functions as a rhetorical device, reinforcing claims of national resilience, institutional competence, and sovereign authority.[271] [272]

This performance raises profound questions of democratic legitimacy. In highly securitized Olympic environments, to what extent are citizens participants in the governance of security, and to what extent are they merely objects of it? Is consent to surveillance implicit, coerced, or

[267] United Kingdom, *Project CONTEST*.
[268] United Kingdom, *London 2012 Olympic and Paralympic Safety and Security Strategy*, March 2011.
[269] République française, *Loi n° 2023-380*, 20 mai 2023.
[270] Faucher and Boussaguet, *The Politics of Symbols*.
[271] DGSI, *Security in the Name of Festivity*.
[272] Cour des comptes, *Rapport complémentaire au Parlement.*

bypassed altogether in the name of the “greater good”? In London, surveillance was largely ambient and integrated into daily urban rhythms. In Paris, it is explicit, experimental, and highly centralized, turning public space into a site of continuous visual and algorithmic scrutiny.

Crucially, the logic of Olympic securitization does not end with the Games. The justifications used to frame threats and pass emergency measures often leave enduring legal and institutional footprints. In the UK, the legacy of CONTEST has been a model of institutionalized counterterrorism that evolved through public debate and bureaucratic layering. In France, the legacy risks becoming one of executive exceptionalism, where policy innovation in crisis settings becomes the default method of governance.

In both countries, threat framing is not just about defining enemies or anticipating violence. It is about legitimizing power, shaping public expectations, and redrawing the boundaries of acceptable state behaviour. Olympic security becomes a laboratory for governance, a stress-test for democratic institutions, and a performative site where the relationship between citizens and the state is temporarily, and perhaps permanently, redefined.

B. Technology and Legal Frameworks

In modern Olympic security planning, technology and law do not merely support security, they constitute it. Surveillance infrastructure, data-processing algorithms, and emergency legal instruments are not peripheral to security; they are its operational substrate. This section compares how the United Kingdom and France mobilized technological systems and legal frameworks to define, detect, and deter threats. Drawing on national legislation, EU regulation, civil society critiques, and governmental technical reports, it reveals how legal architecture and technological experimentation intersect public space, citizenship, and democratic norms during mega-events.

Foundations: National Legal Frameworks and Constitutional Norms

Olympic security regimes have always been rooted in national legal cultures as a way to show the nation's political power around the world. For example, in the UK, the response to 7/7 London bombings and the lead-up to London 2012 took place within the framework of the Regulation of Investigatory Powers Act from 2000 (RIPA) as well as the Anti-Terrorism, Crime and Security Act from 2001, both of which authorized expanded surveillance, data retention, and the interception of communications under conditions of judicial oversight.[273] Both of these statutes became the basis for the intelligence-driven architecture of the CONTEST strategy and were operationalized through "soft law" guidelines rather than bespoke Olympic legislation. This means that rather than legislating something new like France's Law No. 2023-380, the British government relied on existing laws and would layers of additional policies that would adapt to Olympic necessities. These new policies would be layered into preexisting regulatory regimes with the control of committee reviews and finally they were often time-limited unless renewed through parliamentary processes.

This approach reflects broader constitutional norms rooted in common law and parliamentary sovereignty, where emergency powers are generally viewed with suspicion unless accompanied by procedural accountability. RIPA[274], for instance, has been revised multiple times following judicial challenges and European Court of Human Rights rulings[275], demonstrating the reactive but bounded nature of British legal adaptation in the security domain. In the run-up to London 2012, this was translated into a legal model that prioritized oversight and proportionality, though not without controversy, especially regarding the Prevent strategy, one of the four pillars CONTEST counterterrorism framework.

In contrast, France's legal response to the security demands of Paris 2024 is codified by Law No. 2023-380, passed in May 2023. This law explicitly legalized the use of algorithmic video surveillance for the Olympic Games, representing a paradigmatic shift in security governance. The law permits the deployment of AI-enhanced systems in public spaces, ostensibly for anomaly detection.[276] Unlike the UK, where surveillance was scaled up through existing

[273] United Kingdom, *London 2012 Olympic and Paralympic Safety and Security Strategy*, March 2011.
[274] U.K. Parliament, *Regulation of Investigatory Powers Act 2000* (RIPA).
[275] Kennedy v. United Kingdom (no. 26839/05, 18 May 2010).
[276] République française, *Loi n° 2023-380*, 20 mai 2023.

instruments, France created a new legal regime that redefined the boundaries of lawful surveillance under the logic of technological experimentation and public safety.

The law was justified on the basis of "national urgency" and the unprecedented nature of Olympic security needs, drawing on a constitutional tradition more open to the use of emergency powers. French constitutional law permits the extension of such powers via parliamentary vote; a mechanism that was used quite a few times after the terrorist attacks that shook France in 2015. This has contributed to the gradual "normalization" of legal exceptionalism, whereby extraordinary measures are repeatedly extended and ultimately embedded in ordinary law.[277]

Critics, including CNIL and civil society groups such as La Quadrature du Net, warn that the adoption of AI surveillance under Law No. 2023-380 risks passing democratic checks and enabling a permanent shift in how public space is policed.[278] [279] Yet the government maintains that the measure is both temporary and proportional, aligning with broader EU regulations such as GDPR and the Artificial Intelligence Act, passed in July 2024, albeit under derogatory clauses permitted during national emergencies.

As a result, the legal foundations of Olympic security reflect distinct constitutional imaginaries: in the United Kingdom, a model of embedded legality and bureaucratic layering; in France, one of statutory innovation and centralized executive authority. These divergent models not only shape the deployment of technology but also determine the conditions under which surveillance becomes normalized, contested, or reversed.

Surveillance Technologies and State-Business Collaboration

For the respective preparations of their Olympics, both London and Paris invested heavily in surveillance infrastructures, however the nature and ambition of these systems differ. In the case of London 2012, surveillance technologies, including CCTV, ANPR, and

[277] Faucher and Boussaguet, *Politics of Symbols*.
[278] CNIL, *Observations de la CNIL sur le laissez-passer*.
[279] La Quadrature du Net, *Algorithmic Video Surveillance, Dangers and Counter-attacks*.

encrypted communication systems, were integrated into pre-existing urban infrastructure and regulated under established oversight mechanisms like the RIPA.[280] These tools were embedded within a legal tradition that emphasized proportionality, procedural review, and incremental extension of surveillance capabilities. Partnerships with the private sector were functional but conservative, primarily aimed at enhancing infrastructure rather than introducing new surveillance paradigms.

On the other hand, Paris 2024 has embraced algorithmic surveillance as a governance innovation. Under Law No. 2023-380, passed in May 2023, the French state authorized the development and use of AI-powered video analysis tools across Olympic venues and transport junctions. These systems are tasked with detecting behavioural anomalies such as sudden crowd formation, abandoned objects, perimeter violations, or irregular motion flows.[281] The firm Wintics was awarded a major role, providing its Cityvision software, which enables real-time behavioural pattern analysis via fixed and mobile cameras. Wintics is a French company specialised in artificial intelligence applied to video feeds in urban settings. Its flagship product, Cityvision, is designed to assist public authorities by analysing footage from surveillance cameras in real time. In the context of the Olympic Games, Cityvision is used to identify behaviours considered 'abnormal', as crowd surges, lingering objects, or non-linear movements, thereby providing predictive alerts to law enforcement and security personnel. With thousands of cameras connected to predictive analytics platforms, this constitutes the largest legally sanctioned rollout of algorithmic surveillance in French history.[282]

According to the CNIL, the French data protection authority, this deployment raises substantial legal and ethical concerns as there is a certain cloud surrounding algorithmic decision-making, undefined thresholds for anomaly classification, inadequate controls over data retention and deletion, and potential overlaps with biometric identification despite formal denials.[283] While the Ministry of the Interior asserts that the system is non-biometric, CNIL and civil liberties watchdogs, including La Quadrature du Net[284] and Amnesty International,[285] warn that

[280] United Kingdom, *London 2012 Olympic and Paralympic Safety and Security Strategy*, March 2011.
[281] République française, *Loi n° 2023-380*, 20 mai 2023.
[282] Wintics, *Cityvision*, 2024.
[283] CNIL, *Observations de la CNIL sur le laissez-passer*.
[284] La Quadrature du Net, *Algorithmic Video Surveillance, Dangers and Counter-attacks*.
[285] Amnesty International France, *JO 2024 : Pourquoi la vidéosurveillance algorithmique pose problème*.

behavioural pattern recognition may act as a proxy for biometric surveillance, particularly when combined with facial recognition databases or law enforcement watchlists.

This legal and technological configuration also exposes a divergence in democratic accountability. Whereas the UK relied on a model of "quiet embedding", enhancing existing tools without disrupting legal norms, France has opted for a model of "legal experimentalism," where the Olympics serve as a testing ground for technological governance. The rollout was authorized under a strict temporal clause, yet critics argue that this "sunset clause" may not prevent normative creep. Historical precedents in France, such as the persistence of post-2015 emergency laws, suggest that so-called temporary measures often become permanent.

Furthermore, the broader context of European regulation complicates the landscape. While GDPR provides a strong baseline for data protection, France has used national security exemptions to justify deviations. The EU's Artificial Intelligence Act, expected to be fully adopted by 2026, would likely classify certain Olympic surveillance applications as "high risk," requiring stronger transparency and accountability mechanisms.[286] Yet the temporary nature of Law No. 2023-380 effectively allows France to operate in a legal grey zone before stricter EU rules come into force.

In sum, London and Paris diverge not merely in the degree of surveillance but in the logic behind its implementation. London 2012 embedded surveillance within existing democratic guardrails and Paris 2024 reframes security surveillance as a domain of legal and technological experimentation, exposing deeper constitutional tensions between liberty, innovation, and national protection It's important to remember that these two systems were put in place at very different times and under very different conditions. London's approach came after the 7/7 attacks and focused on reforming institutions while staying within existing laws. Paris, on the other hand, is dealing with a more complex and digital threat landscape, shaped by years of terrorist attacks, a growing reliance on emergency laws, and rapid advances in surveillance technology.

[286] European Commission, *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM (2021) 206 final, April 21, 2021 (Brussels: European Commission).

Data Governance: From Consent to Automation

The Olympics challenge not only spatial surveillance norms but also data governance protocols. In the European Union, the GDPR applies to all personal data processing, including video surveillance. However, enforcement becomes inconsistent when national security is cited as a justification for exemptions. For example, article 23 of the GDPR allows member states to restrict certain rights and obligations on grounds of public or national security, this creating legal grey zones, particularly during mega-events like the Olympics.[287]

France's Law No. 2023-380 explicitly places Olympic algorithmic surveillance outside the regular GDPR framework, invoking public safety and counterterrorism as overriding priorities.[288] This legal positioning has sparked criticism from digital rights organizations. Amnesty International[289] and Human Rights Watch[290] warn that framing the Games as a special case creates "exception zones" where democratic protections are suspended. Algorithms are allowed to flag and classify public behaviours without consent, and the criteria for these classifications remain opaque, often protected under national security secrecy.

La Quadrature du Net[291] similarly argues that the public has limited resources to challenge surveillance decisions, since algorithmic logic is treated as proprietary or confidential. CNIL, the French data protection authority, expressed concerns that the rollout lacks sufficient guarantees regarding data minimization, retention, and auditability.[292] Although the Ministry of the Interior claims that the system does not involve biometric tracking, civil liberties advocates note that behavioural pattern recognition can function as a proxy for biometric profiling, especially when deployed at scale.

Meanwhile, the EU's proposed Artificial Intelligence Act aims to regulate "high-risk" AI systems, including those used in law enforcement and crowd monitoring.[293] However, the Act is not yet

[287] EDPB, *Guidelines 10/2020 on Restrictions under Article 23 GDPR*.
[288] République française, *Loi n° 2023-380*, 20 mai 2023.
[289] Amnesty International France, *JO 2024 : Pourquoi la vidéosurveillance algorithmique pose problème*.
[290] HRW, *World Report 2024 : France*.
[291] La Quadrature du Net, *Algorithmic Video Surveillance, Dangers and Counter-attacks*.
[292] CNIL, *Observations de la CNIL sur le laissez-passer*.
[293] European Commission, *Artificial Intelligence Act*, COM (2021) 206 final.

fully in force and contains loopholes that member states may exploit through national security exemptions. France's Olympic experiment shows how bespoke, event-specific laws can pre-empt EU-wide protections, potentially creating normative drift before harmonized regulations are established.

In the UK context, by contrast, Olympic security in 2012 operated under a more traditional legal model. Surveillance and data handling were governed by the Regulation of Investigatory Powers Act[294] and the Data Protection Act 1998,[295] that was later superseded by the 2018 version aligned with GDPR principles. RIPA authorized targeted surveillance with judicial or ministerial approval and was criticized by civil liberties groups for enabling secretive mass interception powers. Yet, it still maintained formal mechanisms for judicial review and parliamentary scrutiny.[296]

The UK's Olympic surveillance strategy did not depend on legal exceptions but on scaling up existing powers. MI5 and local police units enhanced data processing and information sharing, but within a regulatory architecture already in place. This contrasts sharply with France's approach, where a temporary Olympic law has allowed novel forms of data processing without pre-existing safeguards.

The divergence reveals deeper constitutional differences: the UK's model prioritized incrementalism and legal continuity, whereas France's approach has relied on speed, centralization, and a willingness to push legal and technological boundaries. As the EU finalizes the AI Act, the legacy of Paris 2024 may influence how future exemptions are negotiated, and whether major events continue to function as laboratories for permanent shifts in data governance.

The Legal Normalization of the Exceptional

[294] U.K., *RIPA 2000*.
[295] U.K., *Data Protection Act 1998*.
[296] Kennedy v. United Kingdom (no. 26839/05, 18 May 2010).

One of the key concerns in both contexts is the persistence of emergency measures. Olympic surveillance powers are often justified as "temporary," but history suggests these powers risk being extended well beyond the Games themselves. The UK's Prevent strategy, introduced in the early 2000s and scaled up during the lead-up to the 2012 Olympics, is a case in point. Initially framed as part of the Olympic counter-radicalization strategy under CONTEST, it has since become a long-term infrastructure of surveillance and social monitoring in schools, universities, and community organizations. [297]

In France, the fate of algorithmic surveillance beyond 2025 remains uncertain, but the signs point toward permanence. The sunset clause of Law No. 2023-380, which mandates the deactivation of AI-enhanced video surveillance at the end of March 2025, is widely perceived as symbolic and many argue that this clause is still in place today. Some have warned us that unless robust legislative and technical rollbacks are enforced, temporary Olympic measures risk setting a precedent for future deployments in other large-scale national events or during public unrest.[298]

This dynamic has been described and considered as being "experimental authoritarianism" meaning a form of democratic governance in which major events are used to test and legitimize exceptional security regimes that might otherwise face political resistance. In such cases, temporary legislation facilitates the creation of technological infrastructure and public acceptance, only to be repurposed later.[299]

This risk of permanence is amplified by the blurring of emergency powers and everyday governance. NGOs such as La Quadrature du Net[300] and Amnesty International[301] argue that this creates a legal grey zone in which democratic principles are suspended or diluted. As algorithmic systems operate with limited transparency, under national security protections, democratic oversight mechanisms struggle to respond in real time.

Moreover, both the UK and France have shown that once a surveillance infrastructure is in place, be it CCTV networks, algorithmic analytics, or counter-radicalization pipelines, it is rarely

[297] United Kingdom, *London 2012 Olympic and Paralympic Safety and Security Strategy*, March 2011.
[298] Cour des comptes, *Rapport complémentaire au Parlement.*
[299] Faucher and Boussaguet, *The Politics of Symbols*.
[300] La Quadrature du Net, *Algorithmic Video Surveillance, Dangers and Counter-attacks*.
[301] Amnesty International France, *JO 2024 : Pourquoi la vidéosurveillance algorithmique pose problème*.

dismantled. Instead, it is adapted to new contexts, feeding a cycle in which the "exception" becomes the "new normal." In this way, the Olympics function as governance laboratories, testing not just technologies, but public tolerance and the resilience of constitutional limits.

Implications for Civil Liberties and Democratic Oversight

Olympic security is no longer just a technical challenge; it is a constitutional stress test. The technological systems used in London were embedded but contested and in the case of Paris, they are experimental but widely accepted. This difference reflects how each country's legal and political traditions shape public attitudes toward surveillance and state power.

In the UK, Olympic surveillance, while important, was integrated into the existing rule-of-law framework. Parliamentary committees, judicial review, and regulatory oversight by the Investigatory Powers Commissioner's Office (IPCO) provided formal checks and balances. Though controversial, programs like Prevent and RIPA-based surveillance retained a degree of institutional accountability and transparency.[302]

In France, accountability is more fragmented. While the CNIL has issued warnings and recommendations concerning Olympic algorithmic surveillance, its powers are advisory rather than binding.[303] Moreover, the centralization of Olympic security under the Ministry of the Interior has significantly reduced plural oversight. The urgency narrative used to pass Law No. 2023-380, which legalized AI-powered video analysis, also limited parliamentary debate and public consultation.[304]

Public engagement has also diverged. On the one hand, in the UK, Olympic planning involved local councils, civil society forums, and community safety boards. On the other hand, in France, the security architecture for Paris 2024 has been driven top-down, with limited transparency

[302] United Kingdom, *London 2012 Olympic and Paralympic Safety and Security Strategy*, March 2011.
[303] CNIL, *Observations de la CNIL sur le laissez-passer*.
[304] République française, *Loi n° 2023-380*, 20 mai 2023.

over AI contracts, vendor accountability, or operational algorithms. This creates asymmetries not only in governance processes but also in the degree of public understanding and control.

To conclude, what is at stake is not only the immediate safety of the Olympic Games but also the precedent such governance models set for the future. If emergency powers become default tools and experimental technologies are absorbed into routine policing, the Olympics risk becoming catalysts for the transformation of democratic norms. As surveillance becomes both more pervasive and less visible, maintaining meaningful oversight and public debate is essential to preventing the erosion of

C. Governance and Coordination

Security for Olympic Games is not merely about deploying resources, but it is fundamentally about coordination. The scale, complexity, and symbolic value of the Games transform them into testing grounds for national governance models, inter-agency interoperability, and crisis resilience. Both London 2012 and Paris 2024 exemplify how host countries must navigate institutional silos, political pressures, and evolving threat landscapes to produce coherent security responses. This section compares the two governance frameworks, focusing on institutional architecture, inter-agency cooperation, and lessons drawn from past crises and simulations.

Institutional Architectures: From LOCOG to the Préfecture de Police

The institutional architecture behind London 2012 and Paris 2024 represent two contrasting approaches to Olympic security governance, one decentralized and pluralistic, the other centralized and vertically integrated.

In the United Kingdom, the organization of London 2012 rested on a dual governance model that brought together two vastly different worlds. On the one hand stood the LOCOG, charged with the practical task of making the event happen, building venues, coordinating schedules, and ensuring the Games ran smoothly for athletes and spectators alike. On the other hand, however, the responsibility for keeping the event secure never left the hands of the state. The Home Office, working hand in hand with the Metropolitan Police Service (MPS) and other forces, such as the Dorset Police, retained control over all aspects of security. To avoid confusion and ensure clear leadership, the Olympic Security Directorate was set up under Assistant Commissioner Chris Allison, who was appointed as National Olympic Security Coordinator. This structure was essential as the scale of the challenge was quite considerable. As the NPCC later emphasized, the London Games triggered the largest pre-planned policing operation in British history. Fifty-two police forces from across the country contributed officers, who were deployed not only in and around Olympic venues but also at airports, transport hubs, and public gathering spaces, all while everyday policing duties continued elsewhere. In practice, this dual system reflected a simple reality: LOCOG could deliver the Games, but only the state had the authority and resources to safeguard them. [305]

The security structure for London 2012 brought together an unusually wide cast of players: 43 local police forces, the Security Service, also known as MI5, the British Transport Police, private contractors like G4S, and even military units kept on standby. Coordinating so many different organizations was no small task. To keep everyone aligned, senior officers set up daily briefings and put in place a clear chain of command, while the OSSSRA functioned as a common reference point, mapping out the main threats and setting priorities.[306] In theory, this should have created a smooth, unified operation. In practice, however, the coexistence of LOCOG, focused on delivering the Games as an event, and the Home Office-led apparatus, focused on treating it as a matter of national security, sometimes caused friction. Various disagreements surfaced around who controlled resources, who was answerable to the public, and how decisions were made. The most visible example came from G4S: the company had been hired to supply thousands of private security staff but failed to deliver in the weeks before the opening ceremony. The gap

[305] NPCC, *Police Service Delivers Resources for Largest Ever Pre-Planned Operation*.
[306] United Kingdom. Home Department. *Project CONTEST: The Government's Counter-Terrorism Strategy*. Government response to the Ninth Report from the Home Affairs Committee, Session 2008–09, presented to Parliament by the Secretary of State for the Home Department, Command Paper Cm 7703, September 2009.

had to be filled by the military, with soldiers in uniform suddenly appearing at venues and even living in temporary accommodations meant for staff. For many, this episode highlighted the uneasy balance between privatized event management and the state's ultimate responsibility to guarantee security, and showed how, behind the polished image of the Games, coordination was often a daily struggle.[307] [308]

By contrast, Paris 2024 followed a much more centralized state-driven model rooted in the traditions of the French administrative state. Security command and control are housed within the Ministère de l'Intérieur and operationalized through the Préfecture de Police de Paris, which functions as the central node for coordinating police, gendarmerie, intelligence services, known in France as the DGSI, and emergency response actors.

High-level strategic coordination is managed by the SGDSN and the Cellule Interministérielle de Crise (CIC), which are both embedded in the national crisis response framework. Unlike LOCOG, which was a bespoke organising body with limited security oversight, the French system embeds Olympic planning within existing ministerial and territorial hierarchies, drawing on the legacy of the Vigipirate anti-terror doctrine and the state of emergency declared after 2015.[309]

At the heart of France's Olympic preparations sits the Interministerial Delegation to the Olympic and Paralympic Games (DIJOP), a body designed to keep the sprawling machinery of government moving in step. Reporting directly to the Prime Minister, DIJOP acts as a kind of conductor, ensuring that ministries as different as Defence, Justice, Health, Transport, and Sports play in harmony rather than in isolation.[310] It worked hand in hand with the Olympic and Paralympic Council (COP) and the Interministerial Committee for the Olympic and Paralympic Games (CIJOP), both chaired by the Prime Minister, which provides a political stage for overseeing not just the Games themselves but also their longer-term legacy. On the ground, however, the face of Olympic security was Prefect Laurent Nuñez, head of the of the police of Paris. His role has been highly visible, and deliberately so. Each day in the run-up to the Games, Nuñez appeared in front of cameras, leading press briefings, issuing safety updates, and consulting with local authorities and event organizers. At the same time, he overseed the

[307] NPCC, *Police Service Delivers Resources for Largest Ever Pre-Planned Operation*.
[308] Fussey, *Command, Control and Contestation*.
[309] Cour des comptes, *Rapport complémentaire au Parlement.*
[310] République française. *Paris 2024 Olympic and Paralympic Games stakeholders*, Government documentation, published March 21, 2024; modified August 6, 2024.

massive logistical task of deploying around 30,000 officers across the capital on a daily basis, with numbers swelling to 45,000 for the opening ceremony.[311] For Parisians, this meant seeing uniformed officers and gendarmes at every corner, from train stations to fan zones, an unmistakable reminder of the state's presence. Nuñez's leadership illustrates the dual role of the Préfecture de Police in this context: it is both the operational commander managing thousands of moving parts, and the symbolic custodian of public order, tasked with reassuring citizens and projecting calm authority. In many ways, his highly public profile embodies the French state's choice to place security front and centre, making it not just an operational necessity but also a visible guarantee that the Games will be safeguarded.

This vertically integrated architecture allows for faster decision-making and tighter command in times of crisis, but also raises questions about democratic oversight, transparency, and inclusiveness, particularly given the limited role of civil society or municipal actors in the formal governance chain. As Fussey notes in the UK context, pluralism can hinder efficiency but enhance legitimacy. France has opted for the inverse: control over consensus.[312]

Both models reflect broader national traditions. The UK's reliance on a mixed ecosystem of public and private actors mirrors its liberal governance ethos, while France's reliance on state institutions embodies its Jacobin heritage. These choices have practical implications not just for security delivery, but for how the Games are perceived by the public, international observers, and human rights groups.

Inter-agency Coordination and Protocols

The UK developed the OSSSRA as a living document identifying potential threats and mitigation strategies.[313] As a result, OSSSRA served not only as a technical tool but as a platform for horizontal coordination between police forces, intelligence agencies, emergency responders, and private contractors. Daily coordination meetings, integrated contingency

[311] Associated Press. *Paris police chief outlines security measures for Olympics*. 2024.
[312] Fussey, *Command, Control and Contestation*.
[313] United Kingdom, *Project CONTEST*.

planning, and joint exercises promoted coherence across agencies. Therefore, OSSSRA helped break down silos and ensured that strategic intelligence was translated into operational preparedness. [314]

This cooperative approach extended to scenario testing and simulation drills. Before the start of the 2012 Olympics, the city of London ran a wide array of simulation exercises including cyberattacks, mass casualty events, and chemical threats. These simulations revealed coordination gaps and tested communication flows, contributing to an overall strengthening of institutional response capacity. The National Audit Office highlighted how inter-agency rehearsal helped optimize logistics and security response timing, while also ensuring that different layers of government could act cohesively in the event of a major incident.[315]

France has adopted a similarly robust approach but within a much more centralized framework. Inter-agency cooperation revolves around the CIC, the DGSI, the Gendarmerie, and the Paris Préfecture. Strategic coordination is provided by the DIJOP, which acts as a hub aligning ministries such as Defence, Justice, and Health. Operational command resides with the Préfet de Police, enabling rapid mobilization and decision-making authority during crises.

Pre-established protocols for threat escalation and event management are at the heart of France's approach, reflecting institutional learning from past emergencies such as the Bataclan attacks and the Yellow Vest protests. Paris 2024 has also implemented an extensive simulation programme. According to the Cour des Comptes, over 50 full-scale drills were conducted in advance of the Games, testing responses to drone incursions, chemical and radiological threats, stampedes, and failures in AI-assisted surveillance systems.[316]

Simulation exercises were also essential. London 2012 ran large-scale simulations, including cyber drills, counter-terrorism scenarios, and public health emergencies. These exercises were instrumental in building inter-agency trust and refining crisis leadership, particularly within public health and emergency preparedness domains. The drills were not just technical rehearsals but also vehicles for institutional learning, enabling different agencies to familiarize themselves with command hierarchies and communication protocols in high-pressure

[314] Fussey, *Command, Control and Contestation*.
[315] National Audit Office, *Post-Games Review*.
[316] Cour des comptes, *Rapport complémentaire au Parlement.*

environments. These exercises helped expose gaps in preparedness and coordination, especially in scenarios involving multi-agency convergence and cascading risks.[317]

While the UK emphasized coordination through decentralized partnerships and institutionalized flexibility, France has prioritized hierarchical clarity and strategic centralization. Each model reflects national traditions: one oriented toward plural cooperation, the other toward unified command. Nevertheless, both demonstrate the importance of institutional rehearsal and shared threat modelling in managing Olympic-scale risks.

Crisis Response and Resilience Building

The 7/7 London bombings, occurring just one day after the city won its Olympic bid, profoundly shaped the UK's approach to crisis response and security coordination. These attacks exposed critical gaps in emergency preparedness and inter-agency communication, leading to a series of institutional reforms. Reports from the Intelligence and Security Committee and the National Audit Office emphasized the urgent need for real-time data sharing, unified command structures, and pre-established protocols for rapid mobilization.[318] [319]This became a foundational lesson in crisis governance and directly influenced the OSSSRA, a living document that helped synchronize security actors during London 2012.[320]

Importantly, these changes were not just operational but cultural, embedding habits of joint decision-making and situational awareness across organizations such as MI5, the Metropolitan Police, the London Fire Brigade, and Transport for London. Large-scale drills, including cyber incident simulations and public health emergencies, assessed these collaborative mechanisms under pressure.[321] Mega-events like the Olympics function as stress tests for national crisis

[317] Bistaraki, McKeown, and Kyratsis, *Systems Readiness*, 121.
[318] ISC, *Report into the London Terrorist Attacks*.
[319] National Audit Office, *Post-Games Review*.
[320] United Kingdom, *Project CONTEST*.
[321] Bistaraki, McKeown, and Kyratsis, *Systems Readiness*, 121.

systems, forcing governments to re-evaluate how effectively they can manage "no-fail" operations under the global spotlight.[322]

In France, the trauma of the 2015 Paris attacks similarly functioned as a turning point. The government's response, through legal, institutional, and doctrinal adaptation, was anchored in the logic of "permanent vigilance." This mindset led to the institutionalization of resilience-building frameworks. Paris 2024's security model thus focuses on redundancy, meaning the ability for multiple services to fulfil overlapping roles, inter-agency interoperability, and accelerated deployment of counter-terror assets across dense urban areas. The Paris Préfecture, DGSI, and CIC regularly conduct drills that simulate terrorist attacks, CBRN scenarios, and AI system failures.[323]

Cybersecurity has emerged as a particularly strategic domain. In the face of rising ransomware attacks, information manipulation, and cyber sabotage targeting sporting events globally, French authorities placed strong emphasis on digital hardening. The Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) partnered with key ministries and private technology firms to conduct penetration testing, red-teaming, and live attack simulations in collaboration with the Paris 2024 Organising Committee.[324] This operational preparation was informed by cross-sectoral threat intelligence and the experience of past breaches in major events like the Tokyo 2020 or PyeongChang 2018 Olympics.[325]

Resilience-building has also taken a strategic turn through predictive modelling. France's intelligence and crisis coordination bodies, the DGSI and SGDSN, have developed threat anticipation models combining historical attack data, behavioural analysis, and real-time digital feeds. These systems aim to detect early warning signals of hybrid disruptions, from violent extremism and cyber sabotage to mass protests and disinformation campaigns.[326] This represents a paradigmatic shift from reactive policing toward initiative-taking scenario planning. In this logic, "resilience" is no longer purely about recovery, it is about pre-emption, simulation, and behavioural adaptation.

---

[322] Bellavita, Christopher. Changing Homeland Security: A Strategic Logic of Special Event Security. *Homeland Security Affairs* 3, no. 3 (2007).
[323] Cour des comptes, *Rapport complémentaire au Parlement.*
[324] Elgan, *How Paris Olympic Authorities Battled Cyberattacks*.
[325] Nesser and Nasr, *The Threat Matrix Facing the Paris Olympics*.
[326] SGDSN, *Summary of the Information Threat*.

The approach of Paris 2024 can thus be seen as part of a broader European shift toward algorithmic governance and anticipatory security, where crisis response is increasingly mediated through AI tools, dashboards, and simulations. While these tools may enhance agility and response capacity, they also raise concerns around transparency, proportionality, and the human factor in decision-making, especially in real-time high-risk environments.

Civil-Military Interface and Private Sector Roles

The London 2012 Games made visible just how blurred the lines between civilian and military security could become during a mega-event. Military forces were not only mobilized for logistics and specialist roles, but also for high-profile defensive measures. As a result, one of the most and maybe for a great number of people the most controversial was the installation of surface-to-air missile batteries on the rooftops of residential apartment blocks in East London, a move that triggered public protests and sharpened debates about the militarization of urban space.[327] Beyond these symbolic displays of force, the armed forces were also drawn into venue security. This was not originally the plan. Private security firm G4S had been contracted to provide thousands of guards across Olympic sites, but when the company failed to deliver the promised numbers in the final weeks before the Games, 3,500 military personnel were hastily deployed to plug the gap.[328] The sight of soldiers in uniform conducting bag checks and guarding stadium entrances was jarring for many spectators, while politically the episode became a scandal, casting doubt on the reliance on private contractors for core security functions. The G4S crisis revealed the tension inherent in London's hybrid model: while the state retained ultimate responsibility, it had outsourced critical operational capacity to a private actor that failed under pressure.[329]

Paris 2024 has sought to avoid repeating these mistakes. Instead of entrusting venue security to private contractors on the scale of G4S, French authorities relied heavily on state forces, particularly the Gendarmerie and the Sentinel counter-terror patrols established in the

[327] Crilley, *Urban Militarisation and the 2012 London Olympics*.
[328] Hopkins, Gibson, and Mulholland, *G4S Faces Financial Penalties*.
[329] Fussey, *Command, Control and Contestation*.

aftermath of the 2015 attacks.[330] These forces, long embedded in the French security landscape, were mobilized for crowd control, site protection, and counter-terror readiness, providing both workforce and a visible display of state authority. While private security firms are still present in auxiliary roles, assisting with stewarding and basic screening, the most sensitive functions remain firmly in the hands of state agencies.

Where Paris has leaned more visibly on the private sector is in the technological domain. Instead of contracting private companies that would employ many people and labour to function, it has contracted private expertise, particularly in the form of artificial intelligence surveillance. Firms such as Wintics, with its Cityvision software, have partnered with the Préfecture de Police, the Interior Ministry, and transport police to deploy AI-powered video analytics capable of detecting unattended baggage, assaults, or other "anomalous" behaviours in real time.[331] These partnerships illustrate a shift from the manpower crises of London 2012 to the algorithmic governance of Paris 2024. Yet they also raise contemporary issues: as civil liberties groups have pointed out, the delegation of surveillance to proprietary systems developed by private firms complicates transparency and accountability, since the logic of detection often remains hidden behind commercial confidentiality.

This evolution underscores the broader contrast between the two models. London's experiment with large-scale private contracting collapsed into a late reliance on the armed forces, leaving behind a cautionary tale of over-dependence on the market for national security tasks. Paris, by contrast, has tightened the civil-military interface under state control, drawing on existing doctrines like Vigipirate and the legacy of the state of emergency.[332] [333] [334] But it has simultaneously opened the door to private sector involvement in the technological infrastructure of surveillance. In both cases, the question of who controls security, and on what terms, remains at the heart of the Olympic experiment.

[330] Cour des comptes, *Rapport complémentaire au Parlement.*
[331] Wintics, *Cityvision*, 2024.
[332] United Kingdom, *Project CONTEST*.
[333] Cour des comptes, *Rapport complémentaire au Parlement.*
[334] AP News, *Paris police chief outlines security measures*.

Lessons and Challenges: Toward Adaptive Governance

The experiences of London 2012 and Paris 2024 reveal a common dilemma: how to reconcile rigid hierarchies with the fluid, unpredictable environments of a mega-event. London's security planners invested heavily in tools designed to bridge this gap. The OSSSRA provided a common language for agencies, setting out threat scenarios and calibrating resource levels accordingly.[335] Daily coordination meetings and joint exercises further encouraged horizontal collaboration across the 43 police forces, intelligence services, and private contractors involved.[336] On paper, this seemed a robust system. In practice, however, it faltered when one key actor, G4S, failed to meet its obligations, forcing the military to step in at the last minute. The lesson was stark: no amount of planning can fully compensate for weak links in the chain, particularly when those links are outsourced to private providers.[337]

Paris, by contrast, sought to avoid such fragmentation by relying on a more unitary chain of command. The Préfecture de Police and the Ministry of the Interior serve as central nodes, while interministerial bodies like DIJOP ensure coherence across government. This streamlined system allows for swift decision-making and clear lines of authority. Yet, as observers have noted, it comes with its own risks. A heavily centralized model can close down avenues for feedback and limit the involvement of municipal authorities, NGOs, or local communities in shaping security measures.[338] The danger is that while efficiency is gained, legitimacy and inclusiveness may be sacrificed.

Academic analyses reinforce the idea that resilience in Olympic governance depends less on rigid control than on adaptability. Many have argued that security systems must be able to learn from exercises, incorporate feedback from frontline actors, and adjust strategies in real time.[339] Also, the importance of pluralism, bringing diverse perspectives into the governance chain, not only to anticipate blind spots but also to maintain public trust. In London, adaptive governance emerged in improvisational way agencies responded to the G4S failure, but it was reactive rather than planned. In Paris, simulations and crisis drills have been more systematically built

[335] United Kingdom, *Project CONTEST*.
[336] NPCC, *Police Service Delivers Resources for Largest Ever Pre-Planned Operation*.
[337] Fussey, *Command, Control and Contestation*.
[338] Cour des comptes, *Rapport complémentaire au Parlement.*
[339] Bistaraki, McKeown, and Kyratsis, *Systems Readiness*, 121.

into preparation, yet questions remain about whether civil society voices have been adequately heard in shaping the rules of surveillance and public order.[340]

To conclude, the legacies of both Games will not be measured solely by the absence of major security incidents, but by the governance lessons they leave behind. London highlighted the risks of over-reliance on private contractors; Paris illustrated the perils of over-centralization. Both show that the challenge of governing Olympic security is not simply technical but political: it requires balancing control with flexibility, authority with accountability, and security with democratic values. The true test will be whether these experiments in governance serve as one-off solutions or contribute to a more adaptive, globally transferable model for securing future mega-events.

D. Public Perception and Media Discourse

Public perception and media discourse around Olympic security reveal a lot about how societies respond to exceptional measures implemented for mega-events. Both London 2012 and Paris 2024 involved extensive securitization, but the visibility, legitimacy, and reception of these efforts varied significantly across national contexts. In addition to influencing public confidence, the ways in which security measures were communicated, represented, and debated also reflected broader questions about democratic accountability, urban governance, and the normalization of surveillance.

Public Opinion and Polling

In the United Kingdom, public sentiment around Olympic security during London 2012 was shaped by a mixture of optimism, deference to institutional authority, and underlying

[340] Fussey, *Command, Control and Contestation*.

unease. LOCOG's internal post-Games evaluation suggested that over 80% of visitors and residents felt reassured by the visible security presence, highlighting that for a majority of the public this massive presence of police and military was positive and reassuring despite its unprecedented scale.[341] Furthermore, most attendees appreciated the security operation as proportionate, necessary, and effective, adding that the presence of uniformed personnel, ranging from police officers and military staff to private contractors, provoke and enhanced their sense of safety and reassurance. These findings reflect a wider British political culture that has historically tolerated, and at times embraced, robust security interventions, particularly in the context of the post-7/7 terrorism landscape where resilience and vigilance were consistently emphasized by public authorities. [342]

However, more critical academic voices and media reports questioned the long-term implications of this securitization. Some have observed that while many accepted the security arrangements during the Games, a significant proportion of residents expressed discomfort with the militarization of everyday spaces. Some controversial measures, such as the installation of surface-to-air missiles on residential rooftops, the deployment of 17,000 military personnel, and the extensive use of private security company G4S, became focal points for public debate. Localized protests and legal challenges emerged, particularly in neighbourhoods where residents felt excluded from security decision-making. These tensions were amplified by the G4S staffing scandal, which not only revealed operational deficiencies but also symbolized for many the dangers of outsourcing national security to private actors. Additionally, segments of the London population interpreted the Games as a pretext for reinforcing state control and surveillance under the banner of festive unity and global prestige.[343]

On the other hand, in France, before the Paris Olympics public opinion and voices where much more ambivalent and fragmented. According to Ipsos, a French multinational company that surveys public opinion on social and political issues around the world, only 53% of French citizens expressed interest in the Games, a drop of eight points since late 2023. When prompted about the security and organizational aspects, less than half (47%) expressed confidence in the authorities' ability to ensure the Games would run smoothly.[344] Similarly, confidence in

[341] LOCOG, *London 2012 Official Report, Vol. 3*.
[342] George and Mawby, *Security and the 2012 London Olympics*.
[343] Houlihan and Giulianotti, *Politics and the London 2012 Olympics*.
[344] Ipsos. *Le regard des Français sur les Jeux Olympiques de 2024*.

authorities to manage the security of the opening security on the Seine dropped by 14 points, and only 55% believed adequate measures would be in place across venues and public spaces.

At the same time, the numbers revealed a more cautious public mood, less about enthusiasm and more about watchful scepticism. When asked how they felt about the Games overall, 35% of respondents said they were indifferent and 33% expressed concern, with people living in Greater Paris showing even higher levels of both.[345] This suggests that while there may be moments of national pride, a greater number of French citizens remain uneasy about how security and control were being managed at the time.

Although the Ipsos report did not directly measure attitudes toward surveillance technologies during the Games, these trends parallel the tensions evident elsewhere in French society. The introduction of Law No. 2023-380, which authorized algorithmic video surveillance for crowd and anomaly detection,[346] intensified debates around civic trust, oversight, and temporary powers potentially becoming normalized. Framed as a provisional and innovative measure, critics, especially civil rights organizations and younger urban populations, warned that this legislation could pave the way for permanent surveillance infrastructure embedded across Paris's public spaces.

While the French government consistently framed its security strategy in technocratic and legalistic terms, thus emphasizing efficiency, innovation, and operational necessity, many critics argued that this language concealed the deeper democratic implications of AI-powered surveillance. Statements from the Ministry of the Interior presented tools such as Wintics' Cityvision platform as non-intrusive, facial-recognition-free, and compliant with European data protection standards.[347] Yet this official discourse was met with significant resistance. Advocacy groups such as La Quadrature du Net and Amnesty International France denounced the experiment as a step toward the entrenchment of algorithmic policing in everyday life, particularly in the absence of robust, independent oversight. Their concerns were echoed by some opposition parliamentarians and legal scholars, who pointed to the vagueness of certain provisions in the law, the limited duration of the trial period, and the risk of technological path dependency after the Games.

[345] Ipsos, *Le regard des Français sur les Jeux Olympiques de 2024*.
[346] République française, *Loi n° 2023-380*, 20 mai 2023.
[347] AP News, *Paris Police Chief Outlines Olympic Security*.

These tensions were further reflected in the broader socio-political environment. According to *Le Monde*, the Paris Olympics have reinforced the symbolic centrality of Grand Paris as a "Stade XXL", a vast, securitized urban space shaped by flows of people, data, and resources. While some residents expressed pride in hosting the Games, others voiced concern over the transformation of the city's public space into a zone of control and surveillance. Local associations in the Seine-Saint-Denis area, where much of the Olympic infrastructure is concentrated, warned that the long-term legacy of the Games could include not only new housing and transport but also heightened police presence, expanded camera networks, and algorithmic systems that remain embedded in the urban fabric long after the final medal is awarded.[348]

In both Britain and France, public opinion on Olympic security reflects a clear tension. Most people agree that strong security is essential and central, especially given recent terrorist threats, however many are also uneasy about how far these measures go and who's keeping them in check. Trust in government action seems to come with conditions: people want to feel safe, but they also want transparency, fairness, and reassurance that things will return to normal once the Games are over. In this sense, public debate becomes a key space where the limits and legitimacy of security are constantly being questioned and reshaped.

Media Discourses: Militarisation and Spectacle

British media coverage of London 2012 security was largely supportive, especially in mainstream outlets such as the BBC and The Telegraph. Security efforts that some viewed as too much were typically framed by them as being a necessary and proportionate response to a complex threat environment. The imagery of preparedness, uniformed officers, sniffer dogs, surveillance equipment, was often portrayed as a reassuring thing rather than being something alarming. However, The Guardian provided a much more critical analysis,

[348] *Emeline Cazi,* Comment les JO 2024 ont durablement transformé le Grand Paris en stade XXL*, Le Monde, August 21, 2025.*

particularly in the wake of the G4S scandal.[349] The deployment of 17,000 military personnel, the installation of missile systems on residential rooftops, and the staggering £1 billion spent on security sparked headlines questioning whether the securitization of the Games was justifiable or overreaching.[350]

Academic commentators added depth to these critiques. Rhys Crilley described London's security apparatus as an instance of "urban militarization," what he meant by that was a transformation of public space into a high-security zone of exception. He argued that the Games served not only as a sporting spectacle but also as a symbolic performance of state power, projected through visible surveillance infrastructure, military vehicles, and elite police units.[351] Furthermore, Hunter and MacDonald, in their analysis of 176 official security communications between 2010 and 2012, showed how official narratives fused risk management language with messages about national pride and resilience, creating a discursive terrain where security became a patriotic duty. [352]

By contrast, media coverage of Paris 2024 in France has sparked far more debate. Traditional newspapers like Le Monde, Le Parisien, and Le Figaro often backed the government's message, portraying AI-powered surveillance as a necessary and forward avant-garde response to today's complex security challenges. With this in mind, France was not just keeping the Games safe, it was leading the way in urban innovation. *Le Monde*, for example, described the Olympics as a kind of trial run for algorithmic video surveillance, calling it both a technical experiment and a political risk.[353] However, not everyone was convinced. Investigative outlets like Mediapart and Libération voiced much more scepticism. Mediapart sounded the alarm on Law No. 2023-380, warning that what was sold as a temporary and exceptional measure could quietly become a new normal. Their investigation highlighted serious concerns about how these technologies were introduced, with a lack of public debate, unclear procurement processes, and few safeguards to ensure accountability.[354] For numerous critics and civil society groups, the worry

[349] *The Guardian*, *G4S Fails to Supply Enough Staff*.
[350] Hopkins, Gibson, and Mulholland, *G4S Faces Financial Penalties*.
[351] Crilley, *Urban Militarisation and the 2012 London Olympics*.
[352] Malcolm N. MacDonald and Duncan Hunter, The Discourse of Olympic Security: London 2012, *Discourse & Society* 24, no. 1 (2013): 66–88,
[353] Florian Reynaud and Martin Untersinger, "Paris 2024 : la vidéosurveillance algorithmique à l'épreuve des Jeux olympiques," *Le Monde*, July 23, 2024.
[354] Jérôme Hourdeaux, JO 2024 : l'expérimentation de la vidéosurveillance algorithmique inquiète, *Mediapart*, January 24, 2023.

was not just about the Games, but what comes after, namely, whether these powerful tools will stick around long after the final medals have been awarded.

Outside of France, international media, from Reuters to Forbes, quickly seized on the story, presenting Paris 2024 as more than just a sporting event. For many, it looked like a global experiment in AI-driven security. Headlines asked whether the Olympics were turning into a real-world lab for testing surveillance technologies. Civil society overseers and digital rights groups echoed these concerns, warning that tools introduced "just for the Games" might quietly stick around, especially if they prove effective or convenient for authorities.[355]

Academic observers such as Zatsepina and Ludvigsen contributed further critique, noting that while London's militarization relied on human presence and hardware, Paris is entering a new phase of "invisible control" through algorithms, sensors, and predictive analytics. The shift from soldiers in the streets to software in the skies marks a new chapter in the securitization of mega-events, one that raises novel ethical, legal, and political dilemmas that may extend well beyond 2024.[356]

Academic Perspectives on Urban Security Theatre

From an academic point of view, the concept of a "security theatre", was visible to reassure the public more than at addressing actual risks, thus proving particularly pertinent to Olympic security planning. These symbolic actions, while potentially limited in tactical utility, play a key role in projecting state authority and managing public sentiment during mega-events.

Fussey, in his seminal study of London 2012, argued that the Games staged a "performance of control" rather than a demonstration of strategic resilience. The heavily visible deployment of armed personnel, metal detectors, scanners, and crowd barriers were designed to reassure international audiences and domestic publics however it often overshadowed the less visible, yet arguably more effective, intelligence-led efforts managed by MI5 and counter-terrorism

[355] Dal Bello, Hirsch-Hoefler, and Canetti, *AI Video Surveillance*.
[356] Zatsepina and Ludvigsen, *Algorithmic Olympics*.

units. In this reading, Olympic securitisation becomes a "spectacle of assurance," carefully orchestrated to produce emotional and symbolic effects rather than only practical outcomes.[357]

Olympic host cities have been conceptualized as being "fortress spaces", where urban openness and democratic fluidity are temporarily suspended in favour of tightly controlled zones of security. They argue that these zones, although justified by threat perception, reflect a broader shift toward neoliberal governance, where the image of a secure, orderly city is commodified for global consumption. Surveillance, in this context, is as much about optics as it is about safety.[358]

The Paris 2024 Games presented a new iteration of this logic, one less grounded in physical militarization and more centred on algorithmic governance. Visible hardware such as scanners and patrols was increasingly supplemented by AI-powered video analytics, anomaly detection software, and integrated data dashboards. These technologies form a subtler, less immediately visible "security theatre," one that performs reassurance not through physical presence but through the promise of hyper-efficiency and digital omnipresence.

This evolution has been described as a shift toward a "post-human" security regime, in which human operators no longer lead but instead validate machine-generated alerts. This transition implies not just technical efficiency but a reconfiguration of accountability: decisions are pre-processed by algorithms, often based on opaque or proprietary criteria, reducing both transparency and public understanding of how surveillance decisions are made. In this sense, algorithmic security becomes performative in a new way, meaning its legitimacy derived not from visibility, but from the appeal of technological neutrality and necessity. [359]

Boyle and Haggerty reinforced the view that mega-events like the Olympics serve as testing grounds for surveillance innovation.[360] Furthermore, they argued that host cities became "laboratories of control", where temporary states of exception permit the use of technologies and legal measures that would otherwise face resistance in peacetime governance. They suggested that these dynamics produced a choreographed spectacle of safety, wherein risk is continuously framed and managed to reinforce state competence and control.

[357] Fussey, *Command, Control and Contestation*.
[358] Houlihan and Giulianotti, *Politics and the London 2012 Olympics*.
[359] Zatsepina and Ludvigsen, *Algorithmic Olympics*.
[360] Boyle and Haggerty, *Planning for the Worst*.

These scholarly perspectives were essential as they challenged neutrality often attributed to Olympic security planning. Whether through physical deployment or algorithmic surveillance, the Games offer a platform to rehearse new forms of governance, ones that may outlast the event itself. In this view, security theatre is not merely symbolic: it is constitutive of broader shifts in how cities are governed, how rights are balanced against risk, and how the boundaries of acceptable public oversight are continuously renegotiated.

Legacies and the Normalization of Security Exceptionalism

Both London 2012 and Paris 2024 have demonstrated how Olympic security strategies often outlast the events themselves, shaping long-term governance frameworks and altering the boundaries between exceptional and everyday security practices. For example, in the UK, the security infrastructure and coordination mechanisms designed for London 2012 left a lasting imprint. The National Audit Office reported that innovations introduced for the 2012 London Olympics, such as integrated command structures and enhanced inter-agency collaboration, were later adopted and used for major national events, including royal ceremonies and high-risk football matches. While temporary infrastructure like checkpoints was dismantled, enhanced CCTV networks, newly formalized crisis protocols, and private-public security partnerships became embedded into routine security planning. [361] [362]

Similar patterns are beginning to emerge in France after the 2024 Olympics, albeit with a more technologically driven edge. The Paris 2024 Games were the first Olympic event to legally authorize the use of AI-powered video surveillance, enabled through Law No. 2023-380. While framed by the government as a temporary and experimental measure to ensure public safety, the legislation permitted automated video analysis, including crowd anomaly detection and behavioural flagging, until March 2025.[363] However numerous critics have been raised by civil liberties groups and media outlets such as Mediapart, have raised concerns about the potential "post-Olympic drift," warning that tools introduced under the pretext of Olympic security could

[361] National Audit Office, *Post-Games Review*.
[362] Fussey, *Command, Control and Contestation*.
[363] République française, *Loi n° 2023-380*, 20 mai 2023.

become permanent fixtures if perceived as effective or politically expedient.[364] Independent authorities like the CNIL (France's data protection agency) have also questioned the long-term implications of algorithmic policing on transparency, bias, and democratic accountability.[365]

More broadly, both Olympic cases have shown that securitisation is not only about threat prevention, but also about perception management. As Coaffee and Fussey argue, mega-events operate as stages for "security theatre," where the visible performance of safety, whether through military deployments or AI dashboards, serves to reassure the public, project state competence, and demonstrate sovereign control. This theatricality blurs the line between function and symbolism, reinforcing the idea that modern urban governance is increasingly choreographed around the management of risk. In this sense, the legacy of Olympic security is not merely infrastructural but discursive: it shapes how public view safety, how institutions define responsibility, and how cities balance openness with control.[366] [367]

E. Comparative Reflections

This last section looks beyond London and Paris to place Olympic security in a wider, global conversation. It shows how host cities are not working in isolation but are increasingly guided by common rules and expectations from the IOC, the EU, Interpol, and the UN. It also traces how security practices have evolved over time, from the heavy militarization of Athens and Beijing to the more subtle but far-reaching algorithmic surveillance in Paris. Finally, it considers how lessons are shared across countries, how post-Games evaluations are carried out (or sometimes avoided), and what this means for the democratic legitimacy and long-term legacy of Olympic security.

[364] Hourdeaux, *JO 2024 : l'expérimentation de la vidéosurveillance algorithmique inquiéte*.
[365] CNIL, *Observations de la CNIL sur le laissez-passer*.
[366] Coaffee, *Evolving Security Motifs*.
[367] Fussey, *Command, Control and Contestation*.

International Security Frameworks for Mega-Events

In recent Olympic games, their organization and securitization have been operated within an increasingly standardized set of international frameworks. Despite the fact that the security apparatus of each host city remains shaped by their national institutions and threat landscape, supranational and international guidelines, such as the IOC to the EU, INTERPOL, UNOCT and the UNODC, play a significant role in shaping planning, legal obligations, and cross-border cooperation.

One of the central elements of international Olympic governance is the Host City Contract made and written by the IOC, which binds the Host City, National Olympic Committee (NOC), and the Organizing Committee for the Olympic Games (OCOG) to a suite of legal, logistical, and security obligations. These contracts function as legally binding agreements that define the operational and ethical framework under which the Games must be organized. In the cases of both London 2012 and Paris 2024, the Host City Contracts laid out clear and detailed expectations to ensure public safety, prepare for emergencies, and coordinate smoothly between different security agencies during the Games. [368] [369] These clauses mandated the host nation not only to secure venues and athletes but also to manage urban security challenges arising from the concentration of small and easy targets, international visitors, and geopolitical visibility of the event.

Historically, early iterations of the Host City Contract focused primarily on the delivery of infrastructure, coordination, and ceremonial obligations. However, after important security crises, especially after events such as 9/11 and Munich 1972, there has been a marked evolution in the need for more security and especially something written directly in the Host City Contract. Modern versions now explicitly include human rights commitments, integrating language aligned with the Olympic Charter that recognizes the indivisibility of security and civil liberties. [370] This shift reflects a broader move toward embedding normative governance principles within

[368] IOC, *Host City Contract, London 2012*.
[369] CIO, *Contrat Ville Hôte – Principes*.
[370] Human Rights Watch. Olympics: Host City Contract Requires Human Rights, *Human Rights Watch*, February 28, 2017.

the event's operational framework, balancing security imperatives with legal and ethical safeguards.

Moreover, these obligations now extend beyond physical security infrastructure to incorporate digital and biometric security protocols, surveillance technologies, cybersecurity awareness, and counter-terrorism strategies. For example, the Paris 2024 Accreditation Terms and Conditions mandate detailed background checks, information-sharing between national intelligence and police agencies, and adherence to EU data protection standards.[371] Accreditation is not merely an administrative process but a tool for initiative-taking threat prevention, with personal data cross-checked against domestic and international databases, a process reflecting enhanced interoperability between national and supranational law enforcement systems.

As a result, the IOC contract serves not just as a governance blueprint, but as a mechanism for security standardization across host nations, reflecting the best international practices and evolving risk landscapes. It also enables the institutionalization of surveillance norms and event-based exceptions, which often outlast the Games themselves and influence future mega-event planning.

Both London 2012, before Brexit, and Paris 2024, as host cities within the European Union framework, have benefited from and contributed to evolving EU-level security architectures designed to manage transnational threats associated with major public events. At the heart of these frameworks is the EU Security Union Strategy (2020–2025), which outlines coordinated policy priorities across member states in areas such as counterterrorism, critical infrastructure resilience, and cybersecurity awareness.[372] These strategic priorities were especially relevant to Olympic-level event planning, where soft targets, cross-border flows, and high geopolitical visibility generate complex security challenges.

Key institutional mechanisms, notably the Standing Committee on Operational Cooperation on Internal Security (COSI), play a vital role in fostering interoperability and real-time intelligence-sharing across policing, border control, and judicial bodies within the Schengen Area. The EU Security Union Progress Report (2024) further elaborates on the refinement of collaborative

[371] Paris 2024 Organising Committee. *Accreditation Terms and Conditions: Olympic Games Paris 2024*. Paris: Paris 2024 – Summer Olympic Games Organising Committee, 2024.
[372] European Commission, *EU Security Union Strategy*, Communication COM (2020) 605 final, 24 July 2020, Brussels.

mechanisms such as Passenger Name Record (PNR) databases, the Schengen Information System (SIS), and the European Criminal Records Information System (ECRIS), each instrumental in pre-emptively identifying potential threats, tracking suspect movements, and ensuring the secure accreditation of Games personnel and attendees.

While London 2012 was not subject to Schengen rules due to the UK's opt-out, it still operated within broader EU frameworks governing the prevention of organized crime, cybersecurity cooperation, and critical infrastructure protection, particularly through engagement with EUROPOL and COSI-backed data platforms. The UK's access to European intelligence streams allowed the enhancement of border screening, criminal profiling, and coordination of operational response strategies, mechanisms that now remain partially condensed post-Brexit.

On the other hand, for Paris 2024, these EU tools are not only retained but enhanced, with France actively participating in joint threat assessments, scenario modelling, and coordinated police operations across member states. Such coordination has been particularly important in the context of evolving terrorism threats, cyberattacks, and disinformation campaigns, as documented by the European Union Agency for Fundamental Rights [373] and the third EEAS Report on Foreign Information Manipulation and Interference[374].

Furthermore, in addition to strategic interoperability, Statewatch's guidelines on major event security provide rough operational advice on public order management, riot control, and the protection of civil liberties during mass gatherings, areas that have attracted scrutiny in both host countries. In London, concerns arose over the policing of protest zones and the deployment of military assets; and in Paris, debates centre on algorithmic surveillance and the potential overreach of law enforcement powers in urban space.[375] [376]

Together, these EU-level frameworks serve not only as a facilitator of cross-border security coordination, but also as a normative force, standardizing risk management procedures while embedding human rights considerations into the planning of high-security mega-events. For both London and Paris, the Olympic Games thus became areas for testing and consolidating EU-

[373] FRA, *Fundamental Rights… Major Sporting Events*.
[374] European External Action Service, *Third EEAS Report on FIMI Threats*.
[375] Statewatch, *Security of the Spectacle*.
[376] Human Rights Watch, *Olympics: Host City Contract Requires Human Rights*.

wide doctrines of collaborative, technologically integrated, and legally bound security governance.

At a global level, a growing body of transnational guidelines and capacity-building programs has helped standardize the security governance of mega-events, extending well beyond the national domain. A key example is INTERPOL's Project STADIA, which emerged in collaboration with Qatar's hosting of the 2022 FIFA World Cup and has since been generalized as a global framework for major event security planning. STADIA's executive summary articulates a modular approach to risk management, integrating threat assessments, crowd modelling, AI-enhanced surveillance, and multi-agency interoperability.[377] These recommendations emphasize not only operational effectiveness, through real-time information exchange and inter-jurisdictional coordination, but also the integration of advanced technologies such as biometrics, video analytics, and digital identity systems within legal constraints.

Within Europe, INTERPOL has played a complementary role alongside EU institutions by supporting counter-terrorism investigations, cyber threat mitigation, and organized crime disruption, functions that are regularly activated during Olympic cycles.[378] For both London 2012 and Paris 2024, INTERPOL contributed through global police alerts, threat briefings, and the deployment of liaison officers, embedding the Games within a broader matrix of transnational law enforcement cooperation.

Alongside INTERPOL, the UNOCT has emerged as a normative actor shaping mega-event security through its "Guide on the Security of Major Sporting Events".[379] Unlike strictly tactical documents, the UNOCT guide places special emphasis on ensuring that security frameworks are sustainable, rights-respecting, and democratically accountable. It promotes a model in which pre-event planning, intra-agency training, and post-event legacy are all subjected to rule-of-law safeguards and public scrutiny. Notably, the guide encourages host governments to avoid excessive securitization and to resist the normalization of emergency powers beyond the event lifecycle, a concern echoed in civil society critiques of both London's and Paris's post-Games surveillance legacies.[380] [381]

[377] INTERPOL, *Project STADIA: Executive Guidance*, 2023.
[378] International Criminal Police Organization (INTERPOL). *INTERPOL and the European Union*.
[379] UNOCT, *Guide on the Security of Major Sporting Events*.
[380] La Quadrature du Net, *Algorithmic Video Surveillance, Dangers and Counter-attacks*.

In practical terms, these international frameworks have helped anchor Olympic security in a matrix of best practices, information exchange protocols, and legal standards. While implementation remains uneven and deeply shaped by national political cultures, the influence of INTERPOL and UNOCT norms can be observed in multiple dimensions of Games-time operations, from international accreditation vetting and border screening protocols to response simulations and public order doctrines. In the case of Paris 2024, these standards also informed the experimental deployment of AI-powered video surveillance, which, while technologically ambitious, was framed by references to international legality and data protection principles, including compliance with the General Data Protection Regulation (GDPR) and the limitations on biometric profiling.[382] [383]

To conclude, while national law enforcement agencies remain operationally dominant in Olympic security, their actions are increasingly shaped, and at times constrained, by a layered architecture of international governance. From the binding expectations of the IOC Host City Contract to EU-level data sharing systems, to global law enforcement guidance from INTERPOL and the UNOCT, these frameworks collectively embed normative and operational expectations into the heart of mega-event planning. As such, Olympic security has become not only a matter of tactical policing, but a litmus test for the balance between public safety, civil liberties, and global cooperation in an era of heightened securitization.

Lessons from Past Olympics: Athens, Beijing, London, Paris

The Olympic Games are often framed as moments of unity and celebration, yet they have increasingly served as crucibles for evolving security practices. When viewed in sequence and through the years, from Athens 2004, Beijing 2008, London 2012, to Paris 2024, a clear trajectory emerges: from reactive to predictive security, from analogue surveillance to AI-driven analytics, and from visible militarization to more discreet but pervasive systems of

[381] Amnesty International France, *Pourquoi la vidéosurveillance algorithmique pose problème*.
[382] République française, *Loi n° 2023-380*, 20 mai 2023.
[383] EU, *Regulation (EU) 2016/679 (GDPR)*.

control. Each host city became, in its own way, a laboratory for securitizing the modern metropolis.

Athens 2004 marked a turning point. It was the first Summer Olympics held after 9/11 and coincided with heightened fears following the 2004 Madrid train bombings. Greece spent over $1.5 billion on security, at a time a record that outdistanced every other[384] with NATO support, aerial surveillance, and over 70,000 personnel deployed.[385] The scale of the operation overwhelmed local structures and created tensions between imported security doctrines and domestic civil liberties. Post-Games evaluations noted a lack of democratic oversight and limited long-term planning, as much of the surveillance infrastructure was dismantled soon after.[386]

Beijing 2008 took securitisation to an entirely different level, displaying a model of state-centric, pre-emptive control within an authoritarian context. The Chinese government deployed 100,000 security agents and installed an estimated 300,000 surveillance cameras in Beijing alone.[387] This system has been described as "security urbanism," where public spaces were reshaped to reflect political priorities. Activists and journalists were harassed or silenced, revealing the darker side of Olympic security when civil society is absent or suppressed. Surveillance technologies trailed during the Games were not removed but rather absorbed into China's burgeoning digital governance apparatus, serving as a clear precursor to the current model of mass data policing.[388]

By contrast, London 2012 unfolded under the lens of liberal democratic scrutiny yet still exhibited a sharp militarization of urban life. The city had already been scared by the 2005 7/7 bombings, which directly shaped the Olympic Security Strategy.[389] Over 18,000 security personnel were deployed, alongside warships on the Thames, Typhoon jets on standby, and surface-to-air missiles installed on residential rooftops.[390] [391]Public unease was palpable, especially after private security contractor G4S failed to meet staffing obligations, prompting

[384] Samatas, *Security and Surveillance in the Athens 2004 Olympics*, 225.
[385] Brianas, *NATO, Greece and the 2004 Summer Olympics*.
[386] Samatas, *Security and Surveillance in the Athens 2004 Olympics*, 225.
[387] Human Rights Watch, *China: Crackdown Violates Olympic Promises*.
[388]Yu, Klauser, and Chan, *Governing Security at the 2008 Beijing Olympics*.
[389] United Kingdom, *Project CONTEST*.
[390] Crilley, *Urban Militarisation and the 2012 London Olympics*.
[391] BBC News, *London 2012: Olympic Missiles Put in Position*.

last-minute military intervention.[392] [393] Despite official reassurances, media critiques and academic studies point to a performance of security theatre, prioritizing visible deterrence over proportionality.[394] [395] Nevertheless, the UK government did implement institutional reforms post-Games, notably in multi-agency coordination and counterterrorism training for large-scale public events.[396] [397]

Paris 2024 reflects a new phase: one marked less by the sheer visibility of force, and more by the quiet omnipresence of algorithms. Under Law No. 2023-380, France authorized, for the first time, the experimental deployment of AI-driven video surveillance in public spaces, a move both groundbreaking and controversial.[398] These systems, notably Wintics' "Cityvision" software, are designed to detect anomalies like crowd surges, abandoned luggage, or unusual movement patterns, using real-time analytics across 200+ cameras in metro and SNCF stations.[399] Facial recognition remains officially prohibited, yet civil rights groups worry about indirect profiling and the creeping normalization of surveillance.[400] [401] While the Interior Ministry frames this as a pragmatic response to evolving threats, legal scholars argue that the Olympic exceptionalism used to justify such measures risks undermining hard-won safeguards in the long term.[402]

Taken together, these four editions of the Games reveal both convergence and divergence. What unites them is the logic of securitisation: the belief that exceptional risks justify exceptional measures. From the analogue CCTV grids in Athens to the smart, self-learning cameras of Paris, security has become more anticipatory, more data-driven, and often less visible. However, divergences remain striking. Athens and Beijing operated within limited frameworks of public accountability; London, while democratic, leaned heavily on symbolic militarization and private contractors; Paris represents a shift towards "algorithmic governance," where efficiency and innovation are increasingly prioritized over transparency and debate.

---

[392] Hopkins, Gibson, and Mulholland, *G4S Faces Financial Penalties*.
[393] Committee of Public Accounts, *Post-Games review.*
[394] Fussey, *Command, Control and Contestation*.
[395] MacDonald and Hunter, *Discourse of Olympic Security*.
[396] Strom and Eyerman, *Interagency Coordination*.
[397] LOCOG, *London 2012 Official Report, Vol. 3*.
[398] République française, *Loi n° 2023-380*, 20 mai 2023.
[399] Reynaud and Untersinger, *Paris 2024 : la vidéosurveillance algorithmique*.
[400] La Quadrature du Net, *Algorithmic Video Surveillance, Dangers and Counter-attacks*.
[401] Amnesty International France, *Pourquoi la vidéosurveillance algorithmique pose problème*.
[402] Zatsepina and Ludvigsen, *Algorithmic Olympics*.

This evolution mirrors broader global trends. The shift from reactive to predictive policing, from physical deterrence to algorithmic filtering, signals a redefinition of what it means to "secure" a city. Crucially, the Olympic Games, by their scale, visibility, and symbolic weight, act as accelerators of these transitions. Each of these Olympic Games not only reflects the security culture of its host country but also influences the international security playbook for future mega-events.[403]

Yet there is another important and essential element to consider, and this one is the legacy these events will bring to the host nation. The infrastructure, legal precedents, and institutional habits built for two weeks of sport rarely disappear. In China, the surveillance systems of 2008 fed into its broader model of state monitoring. In the UK, lessons from 2012 reshaped planning for royal events and football stadiums. In France, the March 2025 sunset clause on AI surveillance looms, but whether this is truly a sunset or a sunrise for new norms remains to be seen.[404] [405]

To conclude, the Olympic Games offer a mirror, not only to how societies respond to threats but also to what they are willing to sacrifice in the name of safety. The evolution from Athens to Paris is not just a story of cameras and algorithms; it is a story of power, trust, and the boundaries of democratic governance in an age of permanent vigilance.

Transnational Knowledge Sharing and Evaluation

In the intricate landscape of Olympic security governance, learning from the past has become not merely an option but a necessity and a need to advance towards the future. No host city plans in isolation. Each new edition of the Olympic Games is shaped by a growing transnational ecosystem of shared practices, accumulated expertise, and institutional memory. From London 2012 to Paris 2024 and beyond, national security planners draw from a patchwork of policy documents, intelligence briefs, post-event audits, and academic critiques that cross

[403] Coaffee, *Evolving Security Motifs*.
[404] *Marie de Vergès, Vidéosurveillance : attention à la dérive.*
[405] Church Court Chambers, Navigating Legal Challenges: An In-Depth Review of Paris's Handling During the 2024 Olympic Games, *Church Court Chambers*, 2024.

borders and disciplines. Yet, while the infrastructure for transnational learning is becoming increasingly robust, significant challenges persist, particularly in the realms of transparency, critical evaluation, and the inclusion of civil society perspectives.

At the institutional core of this knowledge-sharing process stand EUROPOL and INTERPOL. Both organisations act as knots in an expanding network of security information exchange, providing host nations with strategic foresight and technical guidance. After each major event, EUROPOL integrates post-Games intelligence into its strategic outlook. Its *Programming Document 2025–2027*, for instance, highlights the emerging risks faced by mega-events, ranging from terrorism and cyberattacks to foreign information manipulation and soft target.[406] These reflections directly shape the operational planning of future hosts by emphasising the need for interoperable threat-detection systems, cross-border coordination, and dynamic risk assessments.

INTERPOL's *Project STADIA*, initially developed in preparation for the 2022 FIFA World Cup in Qatar, offers a more formalised mechanism for knowledge transfer. STADIA has since expanded its scope to include Olympic host cities, providing best-practice toolkits on biometric and algorithmic surveillance, inter-agency cooperation, and incident response coordination.[407] Its value lies not just in its operational guidance but in fostering a shared security vocabulary across jurisdictions. For mega-events that rely on transnational policing and intelligence flows, this harmonisation of language and expectations is vital.

Similarly, the UNOCT plays an important role in promoting normative standards for mega-event security. Its 2021 *Guide on the Security of Major Sporting Events* foregrounds principles of sustainability, human rights, and legacy-conscious planning.[408] These principles have influenced national frameworks, such as France's approach to algorithmic surveillance at Paris 2024, by insisting that security must be both effective and proportionate. In practice, however, such international guidance competes with domestic political imperatives, particularly when public anxiety and electoral pressures encourage more intrusive or opaque security solutions.

[406] EUROPOL, *EUROPOL Programming Document 2025–2027*, adopted by the Management Board of Europol, 10 December 2024; published The Hague, 16 December 2024.
[407] INTERPOL, *Project STADIA: Executive Guidance*, 2023.
[408] UNOCT, *Guide on the Security of Major Sporting Events*.

Academic and policy research networks serve as a complementary and often more critical space for reflection. The UK's Economic and Social Research Council (ESRC) has funded several studies on mega-event governance, including assessments of public perceptions, surveillance infrastructure, and democratic oversight. Scholars like Fussey,[409] Coaffee,[410] and Samatas[411] have offered detailed case studies of how surveillance logics evolve across Olympic host cities, highlighting the interplay between global security templates and local implementation. These analyses not only document technological shifts, such as the move from CCTV to AI-driven analytics, but also interrogate their sociopolitical consequences, including the creeping normalisation of emergency governance.

EU-level initiatives such as the Internal Security Fund (ISF) and thematic forums hosted by the Conference of Peripheral Maritime Regions (CPMR) also contribute to this knowledge ecosystem. These platforms allow law enforcement professionals, policymakers, and private sector partners to share innovations, from predictive policing algorithms to new approaches in crowd control and urban resilience. In the lead-up to Paris 2024, such exchanges included scenario planning workshops and field tests of smart surveillance technologies. However, these gatherings often remain closed circles, with limited external scrutiny or engagement from the public.

Despite these positive trends, the evaluation landscape remains fragmented and uneven. Not all states publish systematic post-Games assessments. While the UK's National Audit Office[412] and Home Affairs Committee[413] offered detailed reviews of London 2012, highlighting both strengths and failures, including the outsourcing debacle involving G4S, France's *Cour des Comptes*[414] has so far only produced preliminary financial and logistical reports. These tend to prioritise cost containment and project management over democratic accountability or civil rights monitoring.

The Paris 2024 Games, in particular, illustrate the tension between security innovation and rights-based scrutiny. The introduction of algorithmic video surveillance under *Law No. 2023-*

[409] Fussey, *Command, Control and Contestation*.
[410] Coaffee, *Evolving Security Motifs*.
[411] Samatas, *Security and Surveillance in the Athens 2004 Olympics*, 225.
[412] National Audit Office, *Post-Games Review*, HC 794.
[413] Committee of Public Accounts, *Post-Games review.*
[414] Cour des comptes, *Rapport complémentaire au Parlement.*

380 provoked criticism from digital rights advocates such as La Quadrature du Net[415] and Amnesty International[416], who warned of a slippery slope toward permanent mass surveillance. Although the law explicitly forbade facial recognition and biometric tracking, critics argue that pattern recognition technologies still risk enabling indirect profiling, especially in the absence of robust public oversight.[417] Yet, the institutional response to these concerns has been limited, and the specially mandated evaluation committee has remained largely silent in the public domain.

This asymmetry in evaluation, where technical performance metrics are prioritised while social impacts are overlooked, risks distorting our understanding of what constitutes a "successful" Olympic security operation. Metrics such as the number of incidents prevented or the speed of response may offer a sense of operational efficiency, but they tell us little about the broader implications for public trust, freedom of movement, or the lasting governance of urban space. Without integrating rights assessments, community feedback, and long-term legacy studies, post-Games evaluations risk becoming bureaucratic rituals rather than meaningful learning tools.

There is also a deeper paradox at play: while Olympic security governance is increasingly transnational in its inspiration, it remains largely national in its accountability. International institutions may provide models, funding, and technical guidance, but the actual implementation and public evaluation of those measures are deeply shaped by each host country's political culture, legal system, and media landscape. On the one hand, in France, the centralised structure of state authority has enabled rapid security experimentation, such as the deployment of AI-assisted surveillance, without the kind of broad parliamentary debate that might be expected in other contexts. On the other hand, the UK's more pluralistic approach fostered wider political and media scrutiny, though not without its own limitations.

To move from reactive adaptation to proactive transformation, host cities must develop stronger, more transparent, and more inclusive evaluation processes. Initiatives like the United Nations' *"Securing the Legacy"* programme represent a step in this direction. Rather than simply recycling old blueprints, the programme encourages host nations to reflect critically on what

[415] La Quadrature du Net, *Algorithmic Video Surveillance, Dangers and Counter-attacks*.
[416] Amnesty International France, *Pourquoi la vidéosurveillance algorithmique pose problème*.
[417] Marie de Vergès*, Vidéosurveillance : attention à la dérive.*

worked, what didn't, and, crucially, what might be ethically or socially unacceptable going forward.[418] This requires a deliberate shift from viewing security as a purely technical problem to recognising it as a question of governance, legitimacy, and public trust.

In the end, building a resilient and democratically legitimate Olympic security model is not just about protecting a one-time event. It is about ensuring that the extraordinary security apparatus designed for the Olympics does not leave behind an ordinary legacy of surveillance, opacity, and diminished rights. For that, knowledge sharing is essential, but critical evaluation, open debate, and accountability are indispensable.

[418] United Nations Office of Counterterrorism (UNOCT), *Securing the Legacy: Post-Games Debrief* (New York: UNOCT, March 5, 2025).

Part IV – Lessons and implications

This fourth and final part asks a simple question with important and essential stakes: *what did security in London 2012 and Paris 2024 actually leave behind for safety, for trust, and for democracy?* To answer this question we will first take a look at effectiveness through the public's eyes, meaning did people feel safe, and did institutions stay reliable, then we will turn to ethics and oversight, showing how far is too far, and who gets to decide, and in my third and final part I will take a look at policy transfer and recommendations ,seeing what future hosts should copy, fix, or abandon.

A. Effectiveness and Public Trust

The success of Olympic security cannot be judged only by the fact that no attacks took place. Preventing violence is, of course, the basic requirement. But in democratic societies, effectiveness is also measured by whether the public feels safe, whether institutions act transparently, and whether the security system leaves the Games with its legitimacy intact. Looking back at Paris 2024 a year later, and comparing it with London 2012, we can see both similarities and clear differences in how Olympic security shaped public confidence and the credibility of democratic governance after the event.

London 2012: High Stakes, High Trust

Before the start of the London 2012 Olympic Games, public concern over terrorism was acutely very high, as it was shaped by both historical memory and contemporary risk assessments. The traumatic legacy of the 7$^{th\ of}$ July 2005 bombings, which had killed 52 people and wounded hundreds just one day after London was awarded the Games, cast a long shadow over the planning phase. Coupled with the symbolic centrality of many Olympic venues, including the Olympic Park in Stratford and events staged near Westminster and Tower Bridge, there was an acute awareness among the public and authorities alike of the potential for high-

impact attacks. This risk perception was further fuelled by the broader context of post-9/11 global terrorism, as well as ongoing domestic concerns about radicalisation and the threat of so-called "homegrown" actors.

Against this backdrop, the failure of the private security contractor G4S to meet staffing targets just weeks before the Games emerged as a major political scandal. G4S had been tasked with providing over 10,000 security personnel but fell short by more than 3,500, thus provoking widespread media criticism and urgent parliamentary scrutiny.[419] [420] What could have become a debilitating blow to public confidence was mitigated by a rapid and robust institutional response with the mobilisation of over 18,000 military personnel to fill the gap, thus transforming the Olympic security landscape into one of the most visibly militarised in modern British history. As a result, the Home Office, working in conjunction with the Metropolitan Police Service and MI5, activated a pre-established contingency framework, demonstrating a high level of inter-agency preparedness that had been stress-tested through numerous live exercises in the years prior.[421] [422]

These simulations, which included complex attack scenarios, mass-casualty rehearsals, and cybersecurity drills, allowed for a degree of adaptive capacity that proved essential under pressure. The military presence, while controversial in some quarters, was largely accepted by the public, who interpreted it as a sign of decisive leadership and a commitment to safeguarding the Games. Crucially, this swift institutional reaction helped to transform a potential legitimacy crisis into a demonstration of state competence and resilience. It also set the tone for how the Games were subsequently perceived in terms of security: not without flaws, but fundamentally well-coordinated and successfully executed in the eyes of most stakeholders, including the press and international observers.

Public opinion studies have confirmed in most cases this positive impression of security at the London 2012 Games. According to George and Mawby, a clear majority of spectators reported feeling safe and reassured throughout the event. This sentiment was closely tied to the strong visibility of security measures through the presence of uniformed police officers patrolling

[419] Hopkins, Gibson, and Mulholland, *G4S Faces Financial Penalties*.
[420] PAC, *Post-Games Review*.
[421] United Kingdom, *Project CONTEST*.
[422] Burnham, *Multi-Agency Interoperability*.

transport hubs, soldiers stationed at venues, and the unmistakable presence of surveillance infrastructure across the city. Rather than provoking fear or resistance, these displays were widely interpreted by the public as signs of competence and readiness.[423] The symbolic impact of such visibility cannot be overstated, as it offered Londoners and visitors alike a sense that the state was not only vigilant but fully in control. British media coverage reinforced this narrative. In the weeks of the Games, outlets like the BBC and The Telegraph portrayed the security presence not as a militarization of the city but as responsible guardianship of a national celebration. The tone was one of quiet reassurance, with journalists often highlighting the professionalism and calm demeanour of security personnel as part of the "feel-good" Olympic atmosphere. This framing played an essential role in shaping public confidence. The message was clear: the security operation was not just about protection, but about enabling joy, pride, and global attention to unfold without fear. [424] [425]

At a deeper level, this public trust reflected long-standing British attitudes toward security in the post-7/7 era, a context in which visible deterrence had become normalized, even welcomed, in the name of counterterrorism. For a great number of people, the Olympics were a moment when the lessons of past threats were visibly put into practice. In that sense, the Games offered not just athletic achievement, but a kind of collective catharsis: a chance to showcase resilience, unity, and competent public governance in the face of risk.

Post-Games assessments by the National Audit Office and the Public Accounts Committee reinforced the broader perception that, despite logistical hiccups, the London 2012 security operation had been effective. These reports praised the robustness of the multi-agency coordination model, which successfully brought together police, intelligence services, emergency responders, and military units under a unified command structure. The ability of these bodies to collaborate seamlessly, especially under pressure when the G4S shortfall emerged, was cited as a major strength and a marker of institutional resilience.[426] [427]

At the same time, the evaluations did not shy away from highlighting important shortcomings. Financial inefficiencies, inadequate oversight of private sector contributions, and last-minute

[423] George and Mawby, *Security and the 2012 London Olympics*.
[424] Vincent et al., *'We Are GREAT Britain'*, 900.
[425] Zhou et al., *Creating a Competitive Identity,* 872.
[426] National Audit Office, *Post-Games Review*.
[427] PAC, *Post-Games Review*.

crisis management were all noted as areas for improvement. But what made these critiques constructive rather than damaging was their transparency. The British government's willingness to publish detailed post-event reviews, including candid acknowledgments of where systems had faltered, played a vital role in reinforcing public trust. In an era where crisis management often leans toward opacity or deflection, this openness was a signal of democratic maturity, a way of saying that mistakes were made, lessons were learned, and accountability would follow.

For numerous observers, this post-Games transparency became a legacy in itself. It demonstrated that large-scale security operations could be evaluated publicly, not just in terms of cost or threat mitigation, but also in relation to values like accountability, institutional learning, and respect for public scrutiny.[428] In that sense, the London Olympics helped set a precedent, not just for how to secure a mega-event, but for how to speak about security with honesty after the crowds have gone home.

This democratic reflex, what might be described as a form of *institutional self-correction*, helped London emerge from the Olympic situation not only unscathed, but in many ways strengthened. Despite the immense complexity and scale of the security operation, the willingness of public bodies to acknowledge shortfalls and open themselves to scrutiny gave the event a legitimacy that extended beyond technical success. Transparency was not just a post-Games performance; it became part of the governance ethos, reinforcing the idea that even in high-stakes environments, public institutions could be both powerful and accountable. Of course, this did not mean that criticism disappeared. Academic observers and civil society actors raised fundamental questions about the creeping militarization of public space, the expansion of surveillance networks, and the normalization of extraordinary security measures. Scholars such as Crilley and MacDonald and Hunter warned that the Games may have functioned as a "laboratory" for exceptional policing, while on the other hand Giulianotti highlighted the risks of urban securitization becoming a default model. But what stood out in the British case was that these critiques had space to be voiced, debated, and, in some cases, integrated into future planning.

In this way, the London Games set a rare example: not just in how to manage Olympic-scale risk, but in how to remain democratically open while doing so. The legitimacy of the security

[428] PAC, *Post-Games Review*.

operation was not built on silence or uniform approval, but on the visible contestation of ideas—on the idea that security, too, should be part of the public conversation.

Paris 2024: A High-Tech Achievement, a Trust Gap?

In contrast to London 2012, the Paris 2024 Olympic Games unfolded within a significantly more complex and technologically saturated security environment. France, still scarred by the terrorist attacks that took place between 2015 and 2016, approached Olympic security with a dual imperative: prevent mass violence and adapt to emerging threats such as cyberattacks, disinformation campaigns, and misuse of artificial intelligence. In response, French authorities implemented an innovative security model that leaned heavily on predictive surveillance, real-time data flows, and automated anomaly detection.[429] The system drew upon a vast ecosystem of institutional knowledge, including lessons disseminated through EUROPOL, INTERPOL's STADIA framework, and operational intelligence from previous global sporting events.[430] [431]

Technically speaking, the Paris Games were executed without any major public safety incidents. The strategic use of AI-assisted video surveillance, such as Wintics' Cityvision platform, enabled authorities to monitor dense urban environments like La Défense, Gare du Nord, Chatelet Les Halles and Olympic fan zones across Paris with high levels of precision.[432] Crowd surges, abandoned luggage, or abnormal movement patterns were flagged through automated alert systems, allowing for swift intervention. In parallel, French cybersecurity teams, operating under the SGDSN, successfully repelled several hostile cyber intrusions, including attempted disinformation campaigns and phishing attacks linked to international actors.[433] [434] These outcomes reflect the resilience of France's multi-layered security architecture and its capacity for real-time coordination among intelligence, police, and private sector partners.

---

[429] Cour des comptes, *Rapport complémentaire au Parlement.*
[430] INTERPOL, *Project STADIA: Executive Guidance*, 2023.
[431] Prosegur Security, *Security Report: Olympic Games 2024 – Paris*, Intelligence and Foresight Unit, July 2024.
[432] Wintics, *Cityvision*, 2024.
[433] West, *Cyber Threat to Paris 2024 Olympics*.
[434] European External Action Service, *Third EEAS Report on FIMI Threats*.

However, despite this operational efficacy, public trust in the broader Olympic security governance model remained uneven. A central point of contention was the implementation of Law No. 2023-380, passed in April 2023, which authorized and approved the experimental deployment of algorithmic video surveillance during the Games. Though the law explicitly banned facial recognition and biometric profiling, it introduced algorithmic tools for crowd monitoring, object tracking, and behavioral anomaly detection, a move widely criticized by digital rights advocates for its vague boundaries and insufficient safeguards.[435] [436] La Quadrature du Net, alongside other civil society organizations such as the Ligue des droits de l'Homme, denounced the measure as a "trojan horse" for the permanent algorithmic surveillance of public space.[437]

These concerns were amplified by the relative opacity of the deployment process and the limited visibility of the independent evaluation commission tasked with post-Games oversight. According to the Cour des Comptes, interim reviews focused primarily on budgetary control and logistical performance, with scant attention paid to civil liberties or public consent. The legal framework permitted the use of algorithmic video surveillance until March 2025, leaving many citizens uneasy about whether the promised rollback would indeed materialize after the Olympic period.[438]

Mainstream and investigative media captured this duality with striking clarity. While outlets such as Le Monde and Forbes lauded the Games as a technical success, they also gave voice to widespread societal anxiety about the "normalization of the exceptional".[439] [440] Articles highlighted how experimental tools deployed during the Games, though efficient in managing short-term risk, could quietly seep into routine law enforcement, particularly in the absence of robust sunset clauses or public deliberation.

Public opinion surveys further reflected this tension. According to an Ipsos poll conducted in late 2023, 67% of respondents supported the use of surveillance technologies to ensure Olympic security. However, only 42% expressed confidence that these tools would be used responsibly

[435] Amnesty International France, *Pourquoi la vidéosurveillance algorithmique pose problème*.
[436] Dal Bello, Hirsch-Hoefler, and Canetti, *AI Video Surveillance*.
[437] Hourdeaux, *JO 2024 : l'expérimentation de la vidéosurveillance algorithmique inquiète*.
[438] Marie de Vergès, *Vidéosurveillance : attention à la dérive*.
[439] O'Brien, *Paris 2024: French Government Approves Controversial AI Video Surveillance*.
[440] Reynaud and Untersinger, *Paris 2024 : la vidéosurveillance algorithmique*.

and withdrawn after the Games.[441] INSEE's 2024 confidence barometer similarly showed a modest decline in trust toward public institutions during the Olympic period, particularly among younger and digitally literate demographics.[442] This introduction of AI surveillance, even under time-limited legal frameworks, raises profound ethical questions about consent, democratic oversight, and the future relationship between citizens and the digitally governed city.[443]

In sum, while the Paris 2024 Olympic Games succeeded in delivering a technically robust and incident-free security operation, the legitimacy of that operation remains contested. The French model proved capable of harnessing advanced technologies to address evolving threats, but it struggled to maintain public confidence amid growing fears of securitization without sufficient democratic checks. This tension highlights a broader lesson for future host cities: that security effectiveness must be matched by procedural transparency, civil society engagement, and a meaningful commitment to institutional accountability.

Trust as Legacy

What remains once the Olympic flame is extinguished is more than just economic balance sheets or infrastructure legacies, it is the imprint left on public trust and democratic governance. As both London 2012 and Paris 2024 demonstrate, Olympic security does not end with the absence of incidents. Instead, the deeper, more enduring measure of success lies in how citizens judge the balance between safety and freedom, protection and accountability. Trust, in this sense, becomes not just a by-product of security strategy, but one of its core outcomes, and potentially its most fragile.

The London 2012 Games revealed that trust could emerge even in the face of operational failure, provided there was transparency, reflexivity, and institutional responsiveness. When the G4S debacle occurred, it triggered parliamentary inquiries and intense media scrutiny—but rather than eroding public confidence, this democratic reaction reinforced the legitimacy of the

[441] Ipsos, *Le regard des Français sur les Jeux Olympiques de 2024*.
[442] INSEE. *Baromètre de la confiance : vague 2024*. Paris: INSEE, 2024.
[443] Dal Bello, Hirsch-Hoefler, and Canetti, *AI Video Surveillance*.

response. In essence, the British approach to Olympic security proved that fallibility did not need to be hidden; it could be acknowledged, managed, and even turned into an opportunity for institutional learning. [444] [445]

Paris 2024, by contrast, presents a more ambivalent case. While technically successful, the Games unfolded in a climate of contested legitimacy. The deployment of algorithmic surveillance systems, even under formally temporary conditions, provoked ongoing concern among civil society groups, legal scholars, and parts of the general public. Crucially, what was missing was not technological competence but a clear and credible roadmap for democratic control. The opacity surrounding how AI tools were selected, tested, and evaluated post-Games cast a shadow over the otherwise well-coordinated security apparatus.[446] [447] [448]

This difference reflects a broader shift in how public trust is built or losing contemporary security governance. In an age of digital surveillance and algorithmic policing, transparency must be proactive, not reactive. Trust is not earned simply by preventing harm; it must be cultivated through open dialogue, institutional humility, and legal safeguards that go beyond the letter of the law to address the spirit of democratic accountability.

Moreover, trust is not a static measure but a moving target. It varies by generation, social group, and political context. In Paris, the younger and more digitally literate segments of the population expressed particularly strong scepticism about the long-term trajectory of AI governance.[449] Their fears are not abstract. They are rooted in historical memory of state surveillance, of emergency powers that outlived their crises, and of technologies introduced during exceptional moments but never fully dismantled.

The lesson, then, is that legacy must be defined not only in physical or technological terms, but in relational ones. How did citizens feel? Were they included in the conversation? Did they emerge from the Olympic experience more confident in their institutions, or more wary of them? These questions are central to the legitimacy of security governance, and they will shape the political afterlife of each Games far more than any medal count or operational review.

---

[444] PAC, *Post-Games Review*.
[445] National Audit Office, *Post-Games Review*.
[446] Amnesty International France, *JO 2024 : Pourquoi la vidéosurveillance algorithmique pose problème*.
[447] Cour des comptes, *Rapport complémentaire au Parlement.*
[448] Reynaud and Untersinger, *Paris 2024 : la vidéosurveillance algorithmique*.
[449] Ipsos, *Le regard des Français sur les Jeux Olympiques de 2024*.

For future host cities, this underscores the importance of building a culture of democratic reflexivity into security planning from the outset. This includes not only legal sunset clauses and independent oversight bodies but also mechanisms for public feedback, media scrutiny, and civil society participation throughout the lifecycle of Olympic security, from design to deployment to post-Games evaluation. Without such features, even the most efficient systems risk alienating the very public they are designed to protect.

Therefore, Olympic security is about more than safeguarding infrastructure or individuals, it is about symbolically reaffirming the values of the society in which the Games take place. If the Olympics are a global celebration of peace and cooperation, then their security governance must reflect those ideals not just in form, but in substance. London's example shows that openness and accountability can coexist with preparedness and control. Paris' experience reminds us that technological sophistication must never outpace democratic legitimacy.

The real legacy of Olympic security is not how well it worked on the day, but whether people trust what was built in their name, and whether they feel it belongs to a society that values them as more than just subjects of protection.

B. Ethics and Oversight

The securitization of Olympic Games has historically been justified through the prism of extraordinary threat. Yet, as security measures become increasingly technologically complex, the ethical boundaries between necessity, proportionality, and permanence grow ever more blurred. Nowhere is this tension more apparent than in the governance of surveillance. A comparative lens on London 2012 and Paris 2024 reveals divergent trajectories in oversight, public debate, and democratic accountability, underscoring that the question is no longer simply whether surveillance is effective, but whether it is justifiable, transparent, and time bound.

London 2012: Inward-Facing Oversight and the Ephemeral Logic of Surveillance

The London 2012 Olympic Games unfolded within a national security ecosystem that had long integrated surveillance into its standard operating repertoire. In the years following the 7/7 bombings of 2005, the United Kingdom expanded and normalised a robust surveillance infrastructure, anchored in CCTV, inter-agency intelligence sharing, and digital monitoring systems.[450] [451] By 2012, London was already considered one of the most surveyed cities in the world and is still the case today. As a result, the surveillance tools deployed during the Olympics were not experienced by the public as dramatic innovations or legal outliers. Instead, they were largely seen as natural extensions of the UK's established counterterrorism architecture.

This familiarity played a crucial role in shaping public and institutional attitudes toward Olympic surveillance. There was little suggestion that new legal mechanisms were required, nor was there significant public agitation for ethical inquiry or civil rights protections. From airport-style screening and behaviour detection officers in transport hubs to aerial surveillance and data-sharing across national security entities, these measures were operationalised with relatively little societal pushback. As scholars have noted, the very "predictability" of the security regime insulated it from critique, allowing extraordinary powers to be presented as routine and non-contentious.[452]

Importantly, the mechanisms of oversight during London 2012 were largely contained within the state. Accountability processes operated through inward-facing institutions: parliamentary bodies such as the House of Commons Home Affairs Committee and the Public Accounts Committee conducted post-Games reviews, focusing primarily on logistical efficiency, financial management, and operational delivery. [453] [454] While these committees did flag failings, particularly around G4S's inability to deliver sufficient security personnel, their evaluations did

[450] Strom and Eyerman, *Interagency Coordination*.
[451] United Kingdom, *Project CONTEST*.
[452] Fussey, *Command, Control and Contestation*.
[453] Home Affairs Committee, *Olympic Security: Lessons from London 2012*.
[454] National Audit Office, *Post-Games Review*.

not extend to a systemic or philosophical examination of surveillance powers, nor did they seriously explore the potential long-term implications for democratic life.

Other institutional actors such as the Information Commissioner's Office (ICO) and the Independent Police Complaints Commission had jurisdiction over privacy and policing practices, but their roles during the Olympics remained relatively narrow and reactive. There was no existing equivalent to a standing citizen oversight committee or a mechanism for independent civil liberties monitoring during the Games. This stood in sharp contrast to what might be expected in the context of a security deployment of such unprecedented scale and visibility.

Furthermore, while surveillance technologies, while technically advanced and legally consequential, were treated primarily as logistical tools, means to the end of crowd management and risk mitigation. There was little structured debate over how these tools might shape long-term relationships between citizens and the state, or how the Olympics might function as a testing ground for permanent security transformations.

This silence did not go unnoticed in academic and activist circles. Scholars such as Crilley and Giulianotti pointed to the dangers of allowing Olympic security to pass without rigorous democratic scrutiny, arguing that such mega-events often serve as laboratories for the normalisation of exceptional policing. MacDonald and Hunter went further, warning of the creeping militarisation of urban governance, where security logics begin to displace civic ones. [455] These critiques, however, remained peripheral to the dominant institutional narratives of success, safety, and efficiency.

Indeed, one of the defining characteristics of the London 2012 surveillance regime was its ephemerality, especially in the way it was publicly framed. Surveillance was presented as a temporary necessity, proportionate to the scale and symbolism of the event, with few indications that the technologies or tactics deployed would outlive the Games. But this perception belied a more complex reality. Many of the systems tested or expanded during the Olympics, such as inter-agency data fusion centres and facial detection algorithms, laid the

[455] MacDonald and Hunter, *Discourse of Olympic Security*.

groundwork for more permanent integrations into British policing, especially in urban counterterrorism contexts.[456]

The paradox of London 2012, then, is that while surveillance was deeply embedded in the Games' operational fabric, it remained largely invisible in public debate, not because it was hidden, but because it was normalised. The Games benefited from a political environment in which surveillance was not a taboo but an understood expectation. As such, ethical oversight was assumed rather than actively exercised. The result was a mega-event in which public safety was delivered efficiently, but at the cost of critical democratic conversation, a silence that, in hindsight, raises urgent questions about the long-term effects of "successful" securitisation when legitimacy is taken for granted rather than earned.

Paris 2024: Civil Society Pushback and the Algorithmic Turn

In contrast to the more institutionally contained and bureaucratically framed oversight structures seen during London 2012, Paris 2024 became the stage for an unprecedented, and highly contested, experiment in algorithmic governance. The adoption of Law No. 2023-380 marked a crisis in French legal and technological history: for the first time, public authorities were granted explicit legal permission to deploy AVS powered by artificial intelligence in public space, including metro stations, Olympic fan zones, and other high-traffic areas.[457] AVS technologies such as Wintics' Cityvision were rolled out across more than 200 surveillance points to detect real-time anomalies like abandoned luggage, crowd congestion, or sudden aggressive movements, without relying on biometric identification.[458] [459]

Despite government claims that the measures were strictly time-bound and facial recognition was explicitly prohibited, civil society responses quickly turned critical. The deployment was approved without a robust independent impact assessment, and its legal sunset clause, set for March 2025, extended far beyond the duration of the Olympic and Paralympic Games. This

[456] Fussey, *Command, Control and Contestation*.
[457] République française, *Loi n° 2023-380*, 20 mai 2023.
[458] Wintics, *Cityvision*, 2024.
[459] Dal Bello, Hirsch-Hoefler, and Canetti, *AI Video Surveillance*.

temporal overreach, paired with the opacity of implementation procedures, triggered alarm from a broad coalition of rights organisations including La Quadrature du Net, Amnesty International, and the Ligue des Droits de l'Homme.[460] These actors denounced the "experimental framing" of AVS as a legal loophole, arguing it served as a Trojan horse for normalising invasive security technologies without democratic consensus.[461] [462]

Regulatory oversight itself became a site of contestation. France's national data protection authority, the CNIL, issued a series of observations on the Olympic laissez-passer system, a broader digital framework tied to perimeter access and accreditation. In its May 2024 report, the CNIL voiced serious concerns regarding ambiguous limits on data processing, weak guarantees against function creep, and potential violations of data minimisation principles. Crucially, it criticised the lack of transparency in how detection algorithms were calibrated and the absence of meaningful human verification in high-speed decision-making environments.[463] These findings mirrored broader critiques from digital rights scholars, who questioned whether the legal prohibition of facial recognition was sufficient in preventing other forms of indirect biometric profiling or discriminatory algorithmic bias.[464]

This situation led to a more pluralistic but fragmented oversight landscape. Unlike in London, where surveillance oversight was largely procedural and ex post facto, rooted in parliamentary inquiries and institutional review, Paris was marked by pre-emptive legal activism, street-level mobilisation, and sustained pressure from watchdog groups. Public protests and legal challenges gained visibility in both domestic and European spheres. The EU Fundamental Rights Agency and the European Data Protection Board reiterated that democratic safeguards must be built into the design of AI surveillance systems, not retrofitted after deployment.[465] [466]

Post-Games developments have only heightened these tensions. As Le Monde[467] and Brussels Signal[468] reported, certain AVS systems remained active beyond the Games, with suggestions

[460] Ligue des droits de l'Homme. *Les atteintes aux droits et libertés pendant la période des Jeux Olympiques de Paris 2024*, July 26, 2024.
[461] Amnesty International France, *JO 2024 : Pourquoi la vidéosurveillance algorithmique pose problème*.
[462] Zatsepina and Ludvigsen, *Algorithmic Olympics.*
[463] CNIL, *Observations de la CNIL sur le laissez-passer*.
[464] Zatsepina and Ludvigsen, *Algorithmic Olympics*.
[465] FRA, *Surveillance and Human Rights*.
[466] EDPB, *Guidelines 10/2020 on Restrictions under Article 23 GDPR*.
[467] Reynaud and Untersinger, *Paris 2024 : la vidéosurveillance algorithmique*.

that the French government may seek to integrate them into permanent public safety frameworks. Civil society actors interpret this as clear evidence of "mission creep", the gradual institutionalisation of emergency technologies into the everyday machinery of policing. La Ligue des Droit's de l'Homme report added fuel to these concerns, documenting numerous infringements on civil liberties during the Olympic period, including excessive perimeter controls, opaque AI-generated threat alerts, curtailed protest rights, and diminished transparency in public communication.[469]

The political implications are profound. AVS in Paris 2024 did not simply serve as a temporary public safety tool but became a contested symbol of how liberal democracies grapple with the promises and perils of digital policing. Whereas the UK model in 2012 naturalised surveillance through procedural neutrality, the French model in 2024 actively provoked legal and normative disputes. In doing so, it revealed a key paradox of modern security governance: the more technically advanced a system becomes, the more democratically complex it is to legitimise.

The Paris experiment thus stands as both a milestone and a warning. It showcased the potential of AI-powered systems to manage real-time urban complexity during mega-events, but it also exposed deep vulnerabilities in oversight, consent, and trust. As international debates over AVS intensify, from Brussels to Berlin to Los Angeles, Paris 2024 may be remembered not just for its innovation, but for having sparked a crucial ethical and legal reckoning over the future of algorithmic security in public space.

Between Public Safety and Democratic Cost

In the complex arena of Olympic security governance, knowledge sharing has become a defining element of how host nations prepare, adapt, and respond to the challenges of mega-event safety. No host city starts from zero. From London to Paris, national and local actors benefit from a growing transnational ecosystem of policy learning, professional exchange, and institutional memory. Yet, despite these promising developments, considerable gaps remain in

[468] Caddle, *AI Mass-Surveillance System*.
[469] Ligue des droits de l'Homme, *Atteintes aux droits et libertés*.

how knowledge is disseminated, critically evaluated, and applied, particularly in relation to civil liberties and democratic oversight.

At the forefront of formalised knowledge sharing are organisations such as EUROPOL and INTERPOL. After each Olympic Games, both agencies produce internal reviews and situational reports that contribute to regional and global preparedness. EUROPOL's Programming Document 2025–2027 integrates intelligence from past events and sets out priorities for early threat detection, cross-border surveillance, and counter-terrorism cooperation across member states. These documents also reflect on the specific vulnerabilities posed by mega-events, including cyberattacks, foreign information manipulation, and the exploitation of soft targets.[470]

INTERPOL, for its part, leads Project STADIA, which emerged from its partnership with Qatar ahead of the 2022 FIFA World Cup but has since expanded to support future Olympic hosts. STADIA provided a flexible framework of best practices that encompasses biometric and AI technologies, inter-agency coordination, threat modelling, and event-driven crowd dynamics.[471] Its utility lies not just in technical recommendations but in the creation of a shared vocabulary across jurisdictions. This standardisation is particularly valuable for multi-national events like the Olympics, where cooperation across policing, border security, and intelligence must be seamless.

In parallel, the UNOCT has emerged as an advocate for human-rights-centred security governance. Its 2021 *Guide on the Security of Major Sporting Events* underscores the importance of sustainable security legacies, transparency, and the integration of democratic safeguards into operational planning.[472] France has drawn on many of these principles in framing its security strategy for Paris 2024, as evidenced by national debates around proportionality and rights-based oversight of algorithmic surveillance.[473]

Beyond institutional actors, academic and policy networks play a crucial role in the dissemination and critical reflection of Olympic security practices. Research programmes such as the ESRC-funded "Olympic Games Impact" project and the Surveillance Studies Network have generated comparative insights into the sociotechnical systems underpinning Olympic security.

[470] EUROPOL, *Programming Document 2025–2027*.
[471] INTERPOL, *Project STADIA: Executive Guidance*, 2023.
[472] UNOCT, *Guide on the Security of Major Sporting Events*.
[473] République française, *Loi n° 2023-380*, 20 mai 2023.

Scholars like Fussey, Coaffee and Samatas have mapped the spread of surveillance logics, inter-agency collaboration, and the securitisation of public space from Athens to London to Paris. Their work not only documents the tools and tactics deployed but also interrogates their social and political implications.

However, the overall landscape of evaluation is far from complete. One of the key issues is that not all states publicly share post-Games security data. For instance, while the UK's National Audit Office[474] and the House of Commons Home Affairs Committee[475] published extensive reviews of London 2012, highlighting both operational successes and outsourcing failures (notably with G4S), France's Cour des Comptes[476] has so far provided only interim updates. These reports tend to prioritise budgetary oversight and project management, often omitting robust assessments of civil liberties impacts or long-term surveillance legacies.

Moreover, evaluation mechanisms frequently underplay the concerns of civil society. In the case of Paris 2024, the introduction of algorithmic video surveillance under Law No. 2023-380 provoked substantial debate among rights groups such as La Quadrature du Net and Amnesty International. Critics warned of a slippery slope toward the normalisation of AI-based monitoring, despite the law's formal prohibition of biometric recognition. Yet, there has been limited official response to these critiques, and the evaluation committee tasked with post-Games analysis remains largely invisible in the public sphere.

This asymmetry of evaluation, where technical performance is measured but societal impact is not, risks distorting our understanding of what constitutes a "successful" Olympic security operation. Without deliberate efforts to include human rights assessments, community feedback, and longitudinal studies, post-event reviews risk becoming performative checklists rather than genuine instruments of learning.

The paradox, then, is clear. Olympic security has become increasingly transnational in its models and technologies yet remains stubbornly national in its reflexivity and accountability. The international community offers frameworks, resources, and platforms for exchange, but implementation and evaluation continue to be shaped by domestic political cultures and

[474] National Audit Office, *Post-Games Review*, HC 794.
[475] Home Affairs Committee, *Olympic Security: Lessons from London 2012*.
[476] Cour des comptes, *Rapport complémentaire au Parlement.*

institutional preferences. To build a truly resilient and democratically legitimate Olympic security model, future hosts must not only inherit lessons but also interrogate them.

As the United Nations' post-Games debriefing programme, "Securing the Legacy," aims to demonstrate, the goal is not simply to replicate past frameworks but to critically evaluate their relevance, risks, and resonance in new contexts.[477] Only by confronting the blind spots, from transparency deficits to the marginalisation of civil society voices, can mega-event security evolve from a cycle of reactive adaptation to one of proactive transformation.

C. Policy Transfer and Recommendations

The security operations present during London 2012 and Paris 2024 offered a rich and sometimes uneasy playbook for future Olympic hosts. Both events navigated unprecedented security landscapes, from the spectre of terrorism and cyberattacks to growing public scepticism about surveillance and militarisation. Yet their respective successes and shortcomings offer more than cautionary tales: they point to an evolving toolkit for democratic, effective, and transparent security governance at mega-events.

Learning from the Past: Practical Recommendations

One of the clearest takeaways from both London 2012 and Paris 2024 is that mega-event security cannot rely solely on strength or innovation. It must also be adaptable, layered, and visibly accountable. The complexity of modern threats, from lone-actor terrorism to AI-generated misinformation, demands a planning framework that is not only technically robust but politically and socially resilient. Both London and Paris offer useful, if imperfect, models.

[477] UNOCT, *Securing the Legacy*.

London's approach to risk management was distinguished by its early institutional foresight. The development of the OSSSRA gave security planners a dynamic framework for identifying and prioritizing threats across multiple domains such as terrorism, cyberattacks, public disorder, infrastructure failure. Critically, this framework enabled flexible resource allocation that could be recalibrated in real time as threats evolved.[478] This foresight became essential during the now-infamous G4S staffing collapse, where the private contractor failed to provide the promised personnel just weeks before the Games began. Faced with what could have been a crisis of public confidence, the British state was able quickly by deploying 18,000 military personnel, reconfiguring venue security zones, and restoring trust in the overall operation.[479] [480]

The lesson here is not simply one of institutional competence. It is about the importance of building planning systems that can survive failure. London's strategy was not foolproof, but it was resilient: failures were absorbed without compromising the overall mission. The broader implication is that any Olympic host must embed adaptability into its governance model, not just as a reactive tool, but as a structural feature of risk management.

Paris, for its part, displayed a much more disturbing planning model, reflecting the lessons of both London and more recent global mega-events. Rather than betting on a single point of failure, French authorities diversified both their technological and institutional dependencies. Surveillance infrastructure was bolstered by algorithmic video analysis tools like Wintics' Cityvision, designed to detect anomalies in real time, and cyber defence operations were stress-tested in simulation environments to ensure interoperability between the Interior Ministry, cybersecurity agencies, and private partners like WithSecure.[481] [482]While this made the system more technically sophisticated, it also introduced new vulnerabilities—chief among them, the fragility of public trust in the face of opaque decision-making and ethical ambiguity.

The issue of over relying on contractors remains particularly salient. The G4S incident in London is often cited as a cautionary tale in public-private partnerships gone wrong, exposing the risks of outsourcing critical infrastructure to under-regulated actors. It became emblematic of the broader problem of outsourcing accountability, as public scrutiny turned not just on G4S, but on

[478] United Kingdom, *London 2012 Olympic and Paralympic Safety and Security Strategy*, March 2011.
[479] Hopkins, Gibson, and Mulholland, *G4S Faces Financial Penalties*.
[480] PAC, *Post-Games Review*.
[481] West, *Cyber Threat to Paris 2024 Olympics*.
[482] Dal Bello, Hirsch-Hoefler, and Canetti, *AI Video Surveillance*.

the government's lack of oversight.[483] Paris learned from this, at least structurally. Contractor responsibilities were distributed across several entities, and oversight was partially institutionalized through auditing bodies like the Cour des Comptes. However, the use of AI-powered surveillance, while efficient, reintroduced a different kind of opacity. In this case, the "contractor" was not just a company, but a black-box algorithm whose logic was not publicly explainable or contestable.

This highlights a crucial new dimension of Olympic security: accountability must evolve with technology and its advances. In traditional security operations, oversight mechanisms can follow familiar tracks such as budget reviews, post-event audits, or parliamentary inquiries. But algorithmic security demands new forms of scrutiny: How are algorithms trained? Who defines "anomaly"? What biases might be embedded in pattern recognition? These are not technical questions alone, they are deeply political, and they require public-facing governance structures, not just backend reviews.

Indeed, one of the most important lessons from Paris is the value of anticipatory public debate. While the algorithmic surveillance Law No. 2023-380 was controversial, it triggered early and visible engagement from civil society groups like La Quadrature du Net and Amnesty International, as well as formal intervention from CNIL, France's independent data protection authority.[484] [485] Their criticisms based on the absence of meaningful sunset clauses, weak human oversight, and the slippery slope toward permanent surveillance, helped shape ethical concerns into the national spotlight before the Games began.

This contrasts sharply with the British case, where critiques of Olympic surveillance only emerged after the games, and rarely shaped implementation. In that sense, Paris offered a more democratic, if more contentious, model of security governance. Future hosts should consider integrating this "front-loaded accountability" into their planning processes: conducting independent impact assessments, consulting civil society early, and ensuring that oversight bodies have access not only to financial data, but to the inner workings of surveillance technologies themselves.

[483] Booth and Hopkins, *Olympic security chaos*.
[484] Amnesty International France, *JO 2024 : Pourquoi la vidéosurveillance algorithmique pose problème*.
[485] CNIL, *Observations de la CNIL sur le laissez-passer*.

Lastly, transparency is not just about publishing documents. It is about shaping public narratives of legitimacy. London's ability to recover from the G4S debacle was in large part due to its openness: failures were acknowledged, inquiries were held, and lessons were publicized. Paris' challenges, by contrast, were not operational, but relational: many people simply didn't trust that the security tools being used were in their best interest. The lesson is that legitimacy must be *earned*, not assumed, and it is earned through transparency, humility, and the courage to open the black box of modern security.

Toward a Shared Model of Olympic Security?

As the Olympics continue to grow in symbolic and geopolitical significance, a central question emerges: Is there such a thing as a global model for Olympic security meaning one that balances operational effectiveness with democratic legitimacy, and if it is the case, how close are we to building it?

Over the past two decades, a quiet but steady process of international convergence has emerged in the way Olympic host cities prepare for security threats. Institutions like the IOC have become more proactive, embedding human rights clauses into Host City Contracts since 2017 and encouraging dialogue between event organizers and rights-monitoring bodies.[486] The UNOCT, too, has contributed to the implantation of a practical guidance through a toolkit for rights-respecting security governance, for the, 2024 Olympics, helping states reconcile the imperative of protection with the values of democratic accountability.[487]

At a practical level, we have seen repeated reference points. Cities such as Athens, Beijing, London and Paris increasingly embraced strategies built around multi-agency coordination, cyber resilience, and, at least in theory, legal oversight.[488] [489]These elements now form the backbone of any serious Olympic security plan, and their recurrence suggests not just coincidence, but the emergence of the best international practice vocabulary. However, this

[486] CIO, *Contrat Ville Hôte – Principes*.
[487] UNOCT, *Securing the Legacy*.
[488] Yu, Klauser, and Chan, *Governing Security at the 2008 Beijing Olympics*.
[489] INTERPOL, *Project STADIA: Executive Guidance*, 2023.

story does not end with technical alignment as harmonization is not homogenization, and that distinction is crucial to understand.

Olympic security remains deeply entangled with national political cultures, institutional legacies, and societal expectations. In the United Kingdom, the approach has often centred on internal audit culture and post-event reviews, a model shaped by Westminster-style governance and relatively high public tolerance for surveillance under conditions of perceived threat. London 2012 showcased this case: when things went wrong, the system turned inward meaning towards parliamentary committees, audit reports, ministerial accountability. This reflex was bureaucratic and procedural, but largely effective in containing political fallout.[490] [491]

On the other hand, France demonstrates a more adversarial, anticipatory logic. Paris 2024 was governed less by back-end corrections and more by pre-emptive legal challenges, public protests, and vocal civil society engagement. Law No. 2023-380, which introduced algorithmic video surveillance, was met not with silence but with lawsuits, opinion editorials, and public street actions. Furthermore, the oversight mechanisms were different, too: while the UK leaned on existing bureaucratic structures, France brought in constitutional watchdogs, data protection authorities, and external commissions, thus creating an oversight ecosystem that was pluralistic, if also fragmented.

These divergences matter. They show that there is no universal formula for legitimacy, no one-size-fits-all design for public trust. What might be considered acceptable in one country, such as massive military presence on the streets, mass CCTV coverage, might spark outrage in another. And even shared technologies, like AI-assisted video analytics or digital laissez-passer systems, operate in radically different ethical climates, depending on where and how they are introduced.

So, rather than aiming for a singular "Olympic security model," the real opportunity lies in creating a flexible, pluralistic framework of shared principles, one that respects local governance cultures but commits all host cities to certain non-negotiables: legal clarity, democratic oversight, civil liberties protections, and post-Games accountability.

[490] PAC, *Post-Games Review*.
[491] National Audit Office, *Post-Games Review*.

It is important to signal that this is not just an academic ideal. It's a practical necessity. As surveillance tools become more powerful and less visible, and as public trust in institutions wavers across many democracies, security governance must evolve not only to meet threats but to earn legitimacy. This means shifting the conversation from "what works" to also include "what is justifiable, transparent and reversible".

Some promising steps are already visible. The IOC, for instance, has begun partnering more closely with certain UN agencies and human rights organizations, not just to mitigate reputational risk, but to embed standards of conduct into the DNA of the Games themselves. The UNOCT's guide on major sporting events offers a concrete roadmap for integrating security and rights at every planning phase, not after the fact, but from day one.[492] Meanwhile, initiatives like Project Stadia, led by INTERPOL, are helping cities understand how to translate high-level principles into on-the-ground protocols and shared drills.[493]

Still, much work remains. What is missing is not only a more uniform technical standard, but a common ethical compass. Olympic security cannot be judged solely by whether it prevents attacks, it must also be measured by its capacity to uphold democratic norms in moments of exceptional pressure. And this requires more than exporting blueprints. It requires deep contextual awareness, listening to dissenting voices, and learning from failure without burying it.

Ultimately, the Olympic Games are a celebration not just of athletic excellence, but of shared global ideals such as peace, cooperation, human dignity and equality of opportunity for all. Their security governance must reflect those same principles. And while there may never be one single way to "secure the Games," there is a growing consensus about the values that should guide us in doing so. The task now is to translate that consensus into policy, and to ensure that in securing our public spaces, we do not surrender the very freedoms they are meant to represent.

[492] UNOCT, *Guide on the Security of Major Sporting Events*.
[493] INTERPOL, *Project STADIA: Executive Guidance*, 2023.

The Role of Transnational Policy Learning

In the aftermath of each Olympic Games, the security architecture built for weeks of spectacle leaves behind more than just barricades, data trails, and decommissioned surveillance equipment. What remains is experience that is hard-earned, deeply contextual, and often fragmented. Increasingly, this experience is being gathered, analysed, and shared in what could be described as the early stages of a global learning ecosystem for mega-event security governance.

Following Paris 2024, the UNOCT hosted a high-level debrief titled "Securing the Legacy." This initiative aimed not merely to catalogue successes but to engage in a critical assessment of what worked, what fell short, and how those insights could inform future hosts.[494] The discussions went beyond standard operational metrics to include cross-agency coordination strategies, cyber resilience protocols, and the legal and ethical tensions sparked by algorithmic surveillance.

Alongside UNOCT, INTERPOL's Project Stadia has continued to expand its reach. Initially developed in collaboration with Qatar for the organisation of the 2022 FIFA World Cup, Stadia has evolved into a central repository of tools and frameworks designed to support Olympic-level security planning. It offers host countries access to best practice guidelines, threat simulation models, and resources for enhancing inter-jurisdictional cooperation, including in areas like biometric system management and crowd analytics.[495] These developments mark a promising shift toward codifying knowledge in ways that extend beyond the lifecycle of any single Games.

Yet, despite these encouraging efforts, significant blind spots remain. The current architecture of policy learning, while more robust than in the past, continues to underplay a vital dimension: the long-term impact of Olympic security on civil liberties, democratic norms, and citizen trust. Post-Games evaluations tend to focus on technical efficacy, how well systems performed, how quickly threats were neutralized, how smoothly crowd logistics operated. What is often missing from these assessments is a rigorous examination of how the security apparatus reshaped public space, influenced political culture, or redefined the boundaries of state power.

[494] UNOCT, *Securing the Legacy*.
[495] INTERPOL, *Project STADIA: Executive Guidance*, 2023.

These mega-events like the Olympics have functioned as “laboratories of control.” This means that they allow states to trial new forms of surveillance, behavioural monitoring, and emergency legislation under the guise of necessity and national pride.[496] Some of these measures are rolled back once the Games end. But many quietly persist, either through inertia, institutionalization, or public desensitisation. And yet, there are few formal mechanisms, nationally or internationally, to track and interrogate these longer-term consequences.

To build a more accountable and sustainable model of Olympic security, what is needed is not simply more data-sharing, but deeper reflection. A key recommendation is to embed rights-based impact assessments into every phase of Olympic planning, from the early design of risk frameworks to the post-event debriefs. This should not be seen as a bureaucratic add-on but as a core feature of democratic resilience. Ensuring that civil liberties are treated as strategic concerns, rather than afterthoughts, would mark a significant step forward in aligning security governance with the values it claims to protect.

Imagine, for example, if every Olympic host city were obligated to collaborate with an independent oversight body charged with evaluating the societal consequences of the security measures adopted. Such bodies could publish public-facing reports detailing not only the technical outcomes of security operations but also their implications for protest rights, data privacy, and community relations. They could ask and answer questions such as: How were decisions communicated to the public? What rights were suspended or restricted during the Games? Were surveillance infrastructures dismantled after the event, or did they quietly migrate into standard law enforcement use?

There are signs that some of this thinking is beginning to take root. The European Union Agency for Fundamental Rights (FRA) has issued several recommendations urging host states to consider human rights metrics when planning major sporting events. The UNOCT, in its 2021 guide on safeguarding major events, has similarly called for a broader understanding of “security legacy”, not just in terms of hardware and protocols, but in terms of long-term democratic health.[497]

[496] Boyle and Haggerty, *Planning for the Worst*.
[497] UNOCT, *Guide for the Security of Major Sporting Events*.

Still, these initiatives remain largely voluntary. What is missing is an institutional backbone: a permanent, international mechanism capable of consolidating both the operational and ethical lessons from each Olympic cycle. Such a body could provide standardized benchmarks, encourage mutual accountability, and, crucially, shift the global conversation from a reactive to a preventive posture. It would move us from merely identifying lessons to institutionalizing them.

This would also create the space for uncomfortable but essential questions: Did the security measures disproportionately affect certain communities? Were fundamental rights, such as freedom of assembly or movement, meaningfully protected? Were emergency laws ever truly lifted? And if not, what does that say about the balance we are striking between safety and democratic integrity?

These are not abstract questions. This is the case as they cut to the core of what it means to live in a society that values not only protection from harm, but protection from unchecked power. They remind us that the true legacy of Olympic security cannot be measured solely by the absence of attacks or the smoothness of crowd flows. It must be judged by whether the public emerges from the Games more empowered, more trusting, and more engaged with the institutions that govern them.

Ultimately, the future of Olympic security policy learning depends not only on what we share, but how, why, and with whom we share it. If the Olympics are to remain a celebration of international unity and human excellence, then the governance surrounding them must reflect those same ideals. A Games that protects the body but neglects the rights of the citizen leaves behind a fractured legacy. A Games that protects both offers a vision of what democratic security can truly be.

Conclusion:

Throughout the history of mega sporting events, we have seen, and in our case, that the Olympic Games are never just about sports. They are mirrors of the society in which they were organized. They reflect both the pride and the unease of host nations, becoming stages where athletic brilliance and political order are put in the spotlight so intense that even small mistakes can echo widely, sparking political, social, and economic unrest that could reshape how the host nation is seen at home and abroad. More importantly, it is about negotiating the boundaries between freedom and control, about determining which extraordinary measures and decisions society will accept despite potentially endangering society and finally about what remains of the Olympic Flame once the games are over.

London 2012 offered an interesting but contradictory lesson: these games showed us that legitimacy can even endure despite certain massive failures. The G4S debacle, for example, an event where a private security contractor failed to provide 13,700 guards, arguing that they only had 4,000 in place, thus forcing the British government to deploy its military across London.[498] This event could had easily shattered public confidence in Britain's capacity to organise the Olympic Games; however the important parliamentary scrutiny, public accountability and symbolic resilience of such events showed to the world that despite such crisis, the British government was able to turn it into evidence of its adaptability.

Paris 2024, by contrast, uncovered the other side of the coin. In Paris, technological success did not automatically bring democratic legitimacy. Algorithmic video surveillance may have helped deliver safe, incident-free Games in a climate of terrorism, cyber risks, and civil unrest, but its very effectiveness still leaves a shadow today. Was the response proportionate? Would these tools, such as Law n° 2023-380 allowing the use of AVS during Paris 2024, officially set to end in March 2025[499] yet still argued to persist, really be dismantled once the Games were over? Or, as with earlier states of emergency in France, would the 'exceptional' quietly become part of everyday governance?

[498] Booth and Hopkins, Olympic security chaos.
[499] République française, *Loi n° 2023-380*, 20 mai 2023.

Certain civil organization such as La Quadrature du Net[500] and Amnesty International[501] France have warned the French population as well as the world that behind the existing rhetoric of innovation lurked the danger of normalizing opaque, data-driven surveillance. As a result, Paris 2024 succeeded technically but failed politically, showing us that safety without legitimacy is no real victory at all.

Taken together, these two cases have shown a deeper truth: Olympic security cannot be measured by the absence of violence alone. It must be measured in whether it generates and sustains political and social trust. Security systems and their institutions that keep people safe and secure but leave them feeling excluded may win against immediate threats, but they risk losing the deeper battle for trust and legitimacy. On the one hand, London 2012 reminded us that resilience is strengthened by plainness and accountability. On the other hand, Paris 2024 reminded us that technological sophistication, absent transparency and reversibility, can provoke massive suspicion rather than reassurance.

This dynamic is not something that is unique to both these games. As seen previously, the Games have long functioned as sites of securitization, where ordinary risks are dramatized into existential threats demanding extraordinary responses. As a result, this need for securitization transformed them into laboratories of security innovation, where exceptional measures are tested under the banner of necessity before leaking into everyday life. They have also been stages of public perception, where security is measured not just by effectiveness but by experience, whether soldiers on the streets feel reassuring or intimidating, and whether drones and algorithms are seen as protectors of safety or as signs of unwelcome intrusion. Each host city becomes a arena where societies display the fragile balance between freedom and control, celebration and restraint.

For future hosts, the lessons are both simple and demanding. Security must be technologically competent and adaptable, but also visibly accountable, legally bound, and socially legitimate. Precise deadlines fixed before the start of the events, also known as sunset clauses, must truly expire rather than drift into quiet and unnoticeable extensions. Evaluations must grapple honestly with the civil liberties costs of extraordinary measures, rather than leveling them over

[500] La Quadrature du Net, *Algorithmic Video Surveillance, Dangers and Counter-attacks*.
[501] Amnesty International France, JO 2024 : Pourquoi la vidéosurveillance algorithmique pose problème.

in celebratory after-action reports. Contracts with private providers must be transparent, enforceable, and subject to oversight to avoid repeats such as the G4S fiasco. Without such safeguards, Olympic security risks becoming a Trojan horse, quietly turning temporary exceptions into everyday powers. Most importantly, this means recognizing how “threat framings” itself shape these choices thus understanding how the memory of terrorism in London and the specter of hybrid risks in Paris each served to justify very different forms of security governance, with equally different consequences for democratic accountability.

To conclude, the Games are meant to celebrate peace, human dignity, culture and cooperation. If their security governance undermines those very ideals, something vital to those games is lost. The true legacy of Olympic security is not only whether threats were deterred, but whether citizens trust the systems built in their name, and whether those systems reaffirm rather than corrode the democratic values the Olympics claim to embody. London showed that framing terrorism as an existential threat led to exceptional measures but also demanded visible accountability to restore public confidence. Paris revealed that framing risks as diffuse, hybrid, and technological opened the door to innovation but left legitimacy unresolved.

Therefore, this is the unresolved dilemma that Paris 2024 has left behind, and the one that future hosts will inherit. Will they treat Olympic security as nothing more than a shield against risk? Or will they see it as a chance to model a more open, accountable, and democratic form of protection, one that leaves behind not suspicion and surveillance, but confidence, inclusion, and civic pride? The answer will determine not just the future of Olympic governance, but the credibility of democracy itself in an age where security and freedom so often collide.

Appendix:

Abbreviation	Definition
AI	Artificial Intelligence
ANPR	Automatic Number Plate Recognition
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
AP	Associated Press
AWACS	Airborne Warning and Control System
AVS	Algorithmic Video Surveillance
BTP	British Transport Police
CBRN scenarios	Chemical, Biological, Radiological, Nuclear scenarios
CCTV	Closed-Circuit Television
CIC	Cellule Interministérielle de Crise
CIJOP	Comité Interministériel des Jeux Olympiques et Paralympiques
COSI	Standing Committee on Internal Security
CPMR	Conference of Peripheral Maritime Regions
DIJOP	Délégation Interministérielle aux Jeux Olympiques et Paralympiques

DMI	Defence Medical Intelligence
DPIA	Data Protection Impact Assessment
ECHR	European Convention on Human Rights
ECRIS	European Criminal Records Information System
EDPB	European Data Protection Board
EEAS	European External Action Service
ESRC	Economic and Social Research Council
EUROPOL	European Union Agency for Law Enforcement Cooperation
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FIMI	Foreign Information Manipulation and Interference
FRA	European Union Agency for Fundamental Rights
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
INSEE	Institut National de la Statistique et des Etudes Economiques

INTERPOL	International Criminal Police Organization
IOC	International Olympic Committee
IPCO	Investigatory Powers Commissioner's Office
ISC	Intelligence and Security Committee of Parliament
ISF	Internal Security Fund
JTAC	Joint Terrorism Analysis Centre
LOCOG	London Organising Committee of the Olympic and Paralympic Games
MPS	Metropolitan Police Service
MSE	Major Sporting Events
NAO	National Audit Office
NATO	North Atlantic Treaty Organization
NHS	National Health Service
NOC	National Olympic Committee
NPCC	National Police Chiefs' Council
OCOG	Organising Committee for the Olympic Games
OSCE	Organization for Security and Co-operation in Europe

OSD	Olympic Security Directorate
PNR	Passenger Name Record
RAF	Royal Air Force
RCTU	Regional Counter-Terrorism Units
RER	Réseau Express Régional
RFID	Radio Frequency Identification
SGDSN	Secrétariat Général de la Défense et de la Sécurité Nationale
SIS	Schengen Information System
SNCF	Société Nationale des Chemins de Fer Français
UNOCT	United Nations Office on Counter Terrorism
UNODC	United Nations Office on Drugs and Crimes
VIGINUM	Service for Vigilance and Protection against Foreign Digital Interference

Bibliography:

- Agamben, Giorgio. *The Exceptional Life of the State: Giorgio Agamben's State of Exception.* University of Chicago Press, 2005.

https://www1.cmc.edu/pages/faculty/LdelaDurantaye/Agambens_State_of_Exception.pdf

- Amoore, Louise. *Algorithmic War: Everyday Geographies of the War on Terror*. Antipode 41, no. 1 (2009): pp. 49–69.

file:///C:/Users/herau/Downloads/Antipode%20-%202009%20-%20Amoore%20-%20Algorithmic%20War%20%20Everyday%20Geographies%20of%20the%20War%20on%20Terror.pdf

- Amnesty International France. *Jeux de Paris 2024 et surveillance algorithmique : nos préoccupations*. Paris: Amnesty International France, 2024.

JO 2024 : Pourquoi la vidéosurveillance algorithmique pose problème - Amnesty International France

- AP News. *Paris Police Chief Laurent Nuñez Details Security Mobilization for Opening Ceremony*. AP *News*, 2024.

https://apnews.com/article/olympics-security-police-eff374adfb0f7db39513421764ab4b96

- BBC News. *London 2012: Olympic Missiles Put in Position*. BBC News, July 12, 2012.

https://www.bbc.com/news/uk-england-london-18816421

- Bellavita, Christopher**.** *Changing Homeland Security: Shape Patterns, Not Programs.* Homeland Security Affairs, no. 3 (2007).

https://www.hsaj.org/resources/uploads/2022/05/3.3.1.pdf

- Birkett, Paul. *London 2012: Protecting the Olympic Games*. Domestic Preparedness, July 25, 2012.

https://domesticpreparedness.com/articles/london-2012-protecting-the-olympic-games#:~:text=The%20most%20relevant%20terrorist%20outrage,effect%20might%20still%20prove%20lethal.

- Bistaraki, Angeliki, Eammon McKeown, and Ioanna Kyratsis. *Systems Readiness and Crisis Leadership during London 2012*. Public Health 165 (2018) : pp. 119–26.

file:///C:/Users/herau/Downloads/publichealtharticle.pdf

- Blumenau, Bernhard. *The Munich Massacre and Its Aftermath: A Securitization of Mega-Events.* Foundation Pierre du Bois Report No. 8. Pully, Switzerland: Fondation Pierre du Bois, October 2022.

https://www.fondation-pierredubois.ch/wp-content/uploads/2022/10/2022-no8-Blumenau.pdf

- Booth, Robert, and Nick Hopkins. *Olympic security chaos: depth of G4S security crisis revealed*. The Guardian, July 13, 2012.

https://www.theguardian.com/sport/2012/jul/12/london-2012-g4s-security-crisis

- Brianas, Jason J. *NATO, Greece and the 2004 Summer Olympics*. Thesis, Naval Postgraduate School, 2004.

NATO, Greece and the 2w004 Summer Olympics

- British Transport Police. *Archival Notes on 7/7 and Transport Policing Lessons.* BTP Internal Release, 2023.

London bombings of 2005 | British Transport Police

- Burnham, Paul. *Multi-Agency Interoperability at Major Sporting and Sailing Events*. Doha: Josoor Institute, January 2021.

https://knowledgehub.josoorinstitute.qa/wp-content/uploads/2021/01/Multi-Agency-Interoperability-At-Major-Sporting-and-Sailing-Events.pdf

- Cazi, Emeline. *Comment les JO 2024 ont durablement transformé le Grand Paris en stade XXL*. *Le Monde*, August 21, 2025.

https://www.lemonde.fr/economie/article/2025/08/21/les-jo-2024-confortent-le-grand-paris-comme-stade-xxl_6632832_3234.html

- Church Court Chambers. *Navigating Legal Challenges: An In-Depth Review of Paris's Handling During the 2024 Olympic Games.* Church Court Chambers, 2024.

https://churchcourtchambers.co.uk/article/navigating-legal-challenges-an-in-depth-review-of-paris-handling-during-the-2024-olympic-games/

- Commission nationale de l'informatique et des libertés. *Jeux olympiques et paralympiques 2024 : les observations de la CNIL sur le dispositif de laissez-passer*. CNIL, May 13, 2024.

Jeux olympiques et paralympiques 2024 : les observations de la CNIL sur le dispositif de laissez-passer | CNIL

- Coaffee, Jon. *Evolving Security Motifs, Olympic Spectacle and Urban Planning Legacy: From Militarization to Security-by-Design*. *Planning Perspectives* 39, no. 3 (2024) : 637–657.

file:///C:/Users/herau/Downloads/Evolving%20security%20motifs%20%20Olympic%20spectacle%20and%20urban%20planning%20legacy%20%20from%20militarization%20to%20security-by-design.pdf

- Comité International Olympique. *Contrat Ville Hôte – Principes, Jeux de la XXXIIIe Olympiade en 2024*. Signed in Lima, 13 September 2017.

https://stillmed.olympic.org/media/Document%20Library/OlympicOrg/Documents/Host-City-Elections/XXXIII-Olympiad-2024/Contrat-ville-hote-Principes-pour-les-Jeux-de-la-XXXIII-Olympiade-2024.pdf

- Cour des comptes. *L'organisation des Jeux Olympiques et Paralympiques de Paris 2024* : Rapport complémentaire au Parlement. Paris, July 2023.

https://www.ccomptes.fr/sites/default/files/2023-10/20230720-JOP-Paris-2024-complementaire.pdf

- Crilley, Rhys. *Urban Militarisation and the 2012 London Olympics*. E-International Relations, July 2012.

https://www.e-ir.info/pdf/24502

- Culf, Andrew. *The party that never was: capital marks the games at last*. The Guardian, September 2, 2005.

https://www.theguardian.com/uk/2005/sep/02/london.Olympics2012

- Dal Bello, Giulia, Sivan Hirsch-Hoefler, and Daphna Canetti. *AI Video Surveillance at the 2024 Paris Olympics. The Loop*, September 24, 2024.

AI video surveillance at the 2024 Paris Olympics

- Direction Générale de la Sécurité Intérieure (DGSI). *Le plan VIGIPIRATE.* Published June 11, 2022; updated November 26, 2024.

Le plan VIGIPIRATE | Direction Générale de la Sécurité Intérieure

- Direction Générale de la Sécurité Intérieure (DGSI). The *Olympic and Paralympic Games: Security in the Name of Festivity*. Published November 28, 2023; updated November 26, 2024.

The Olympic and Paralympic Games : security in the name of festivity | Direction Générale de la Sécurité Intérieure

- European External Action Service. *Third EEAS Report on Foreign Information Manipulation and Interference Threats: Exposing the Architecture of FIMI Operations*. March 2025. European External Action Service.

https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf

- European Data Protection Board (EDPB). *Guidelines 10/2020 on Restrictions under Article 23 GDPR*. Version 2.0, adopted October 13, 2021.

https://www.edpb.europa.eu/system/files/2021-10/edpb_guidelines202010_on_art23_adopted_after_consultation_en.pdf

- Elgan, Mike. *How Paris Olympic Authorities Battled Cyberattacks and Won Gold*. *IBM Think* (blog), August 23, 2024.

https://www.ibm.com/think/insights/paris-olympic-authorities-battled-cyberattacks-won-gold

- European Commission. *EU Security Union Strategy*. Communication COM (2020) 605 final, 24 July 2020. Brussels.

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605

- European Commission. *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*. COM (2021) 206 final, April 21, 2021. Brussels: European Commission.

https://digital-strategy.ec.europa.eu/en/node/9756/printable/pdf

- European Union Agency for Fundamental Rights (FRA). *Reactions to the Paris Attacks in the EU: Fundamental Rights Considerations*. FRA Paper 01/2015. Luxembourg: Publications Office of the European Union, 12 February 2015.

https://fra.europa.eu/sites/default/files/fra-2015-paper-01-2015-post-paris-attacks-fundamental-rights-considerations-0_en.pdf

- Europol. *Europol Programming Document 2025–2027*. Adopted by the Management Board of Europol on 10 December 2024; published The Hague, 16 December 2024.

https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Programming_Document_2025-2027.pdf

- Faucher, Florence, and Laurie Boussaguet. *The Politics of Symbols: The French Government's Response to the 2015 Terrorist Attacks.* Cogito (Sciences Po), October 27, 2018.

https://www.sciencespo.fr/research/cogito/home/the-politics-of-symbols-the-french-governments-response-to-the-2015-terrorist-attacks/?lang=en

- Federal Bureau of Investigation. *Eric Rudolph*. FBI History—Famous Cases. n.d.

https://www.fbi.gov/history/famous-cases/eric-rudolph

- Fussey, Pete. *Command, Control and Contestation: Negotiating Security at the London 2012 Olympics*. *Geographical Journal* 181, no. 3 (September 2015): 212-223.

https://www.jstor.org/stable/pdf/43868649.pdf

- George, Richard, and Rob. I. Mawby. *Security at the 2012 London Olympics: Spectators' Perceptions of London as a Safe City.* Security Journal 28, no. 1 (November 2013): 1–11.

file:///C:/Users/herau/Downloads/SecurityJournalARTICLE.pdf

- Giulianotti, Richard, and Francisco Klauser. *Security Governance and Sport Mega-events: Toward an Interdisciplinary Research Agenda*. Journal of Sport and Social Issues 34, no. 1 (February 2010).

file:///C:/Users/herau/Downloads/lm.php.pdf

- Houlihan, Barrie, and Richard Giulianotti. *Politics and the London 2012 Olympics: the (in)security Games.* International Affairs 88, no. 4 (2012): 701–717.

https://ciaotest.cc.columbia.edu/journals/riia/v88i4/f_0025559_20909.pdf

- Hopkins, Nick, Owen Gibson, and Hélène Mulholland. *G4S Faces Financial Penalties over Olympic Security Failures*. The Guardian, July 12, 2012.

https://www.theguardian.com/sport/2012/jul/12/g4s-financial-penalties-olympic-security

- Hourdeaux, Jérôme. *JO 2024 : l'expérimentation de la vidéosurveillance algorithmique inquiète*. Mediapart, January 24, 2023.

https://www.mediapart.fr/journal/france/240123/jo-2024-l-experimentation-de-la-videosurveillance-algorithmique-inquiete

- House of Commons Home Affairs Committee. *Olympics Security: Seventh Report of Session 2012–13*, HC 531-I. London: The Stationery Office, 21 September 2012.

https://publications.parliament.uk/pa/cm201213/cmselect/cmhaff/531/531.pdf

- House of Commons Committee of Public Accounts. *The London 2012 Olympic Games and Paralympic Games: post-Games review*. Fortieth Report of Session 2012–13 (HC 812). London: The Stationery Office, 19 April 2013. Ordered printed 18 March 2013.

https://publications.parliament.uk/pa/cm201213/cmselect/cmpubacc/812/812.pdf

- Human Rights Watch. *China: Crackdown Violates Olympic Promises*. Human Rights Watch, February 6, 2008.

https://www.hrw.org/news/2008/02/06/china-crackdown-violates-olympic-promises

- Human Rights Watch. *Olympics: Host City Contract Requires Human Rights*. Human Rights Watch, February 28, 2017.

https://www.hrw.org/news/2017/02/28/olympics-host-city-contract-requires-human-rights

- INTERPOL**.** *Project STADIA: Executive Guidance for Major Event Security.* Lyon, 2023.

file:///C:/Users/herau/Downloads/Executive%20Summary%20to%20Web%2010_2023-1.pdf

- International Criminal Police Organization (INTERPOL). *INTERPOL and the European Union*.

https://www.interpol.int/en/Who-we-are/Our-partners/International-organization-partners/INTERPOL-and-the-European-Union?utm_source=chatgpt.com

- International Olympic Committee. *Host City Contract for the Games of the XXX Olympiad in 2012*. Executed in Singapore on 6 July 2005.

https://www.gamesmonitor.org.uk/files/Host%20City%20Contract.pdf

- Ipsos. *Le regard des Français sur les Jeux Olympiques de 2024*. April 2024. Ipsos.

https://www.ipsos.com/fr-fr/le-regard-des-francais-sur-les-jeux-olympiques-de-2024

- Jennings, Will, and Martin Lodge. *Tools of Security Risk Management for the London 2012 Olympic Games and the FIFA 2006 World Cup in Germany*. Discussion Paper No. 55. London: ESRC Centre for Analysis of Risk and Regulation, November 2009.

https://eprints.lse.ac.uk/36539/1/Disspaper55.pdf

- Kennedy v. United Kingdom, no. 26839/05. Judgment of 18 May 2010. European Court of Human Rights. HUDOC item no. 001-98473.

https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-98473%22]}

- La Quadrature du Net. *Algorithmic Video Surveillance, Dangers and Counter-attacks*. Paris: La Quadrature du Net, 2023.

https://www.laquadrature.net/en/avs/

- Ligue des droits de l'Homme. *Les atteintes aux droits et libertés pendant la période des Jeux Olympiques de Paris 2024*. July 26, 2024.

https://www.ldh-france.org/les-atteintes-aux-droits-et-libertes-pendant-la-periode-des-jeux-olympiques-de-paris-2024/

- London Organizing Committee of the Olympic Games and Paralympic Games (LOCOG). *London 2012: Official Report, Volume 3 – Servicing the Games*. Lausanne: International Olympic Committee (IOC), 2013.

https://stillmed.olympic.org/Documents/Reports/Official%20Past%20Games%20Reports/Summer/2012/ENG/2012-RO-S-London_V3_eng.pdf

- MacDonald, Malcolm N., and Duncan Hunter. *The Discourse of Olympic Security: London 2012*. Discourse & Society 24, no. 1 (2013): 66–88.

https://www.jstor.org/stable/pdf/24441658.pdf?refreqid=fastly-default%3A7780cc82890386fb9737ee981689623e&ab_segments=&initiator=&acceptTC=1

- Marie de Vergès, Léa. *Vidéosurveillance : attention à la dérive post-Jeux olympiques et paralympiques*. Le Monde, September 26, 2024.

https://www.lemonde.fr/idees/article/2024/09/26/videosurveillance-attention-a-la-derive-post-jeux-olympiques-et-paralympiques_6334585_3232.html

- National Audit Office. *The London 2012 Olympic Games and Paralympic Games: Post-Games Review*. HC 794 (Session 2012–13). Report by the Comptroller and Auditor General, presented to Parliament on 5 December 2012. London: The Stationery Office, 2012.

https://www.nao.org.uk/wp-content/uploads/2012/12/1213794fr.pdf

- Neate, Rupert. *G4S profits tumble on Olympics failings*. The Guardian, March 13, 2013.

https://www.theguardian.com/business/2013/mar/13/g4s-profits-tumble-olympics-failings

- Nesser, Petter, and Wassim Nasr. *The Threat Matrix Facing the Paris Olympics*. CTC Sentinel 17, no. 6 (June 2024).

https://ctc.westpoint.edu/wp-content/uploads/2024/06/CTC-SENTINEL-062024_cover-article.pdf

- National Police Chiefs' Council. *Police Service Delivers Resources for Largest Ever Pre-Planned Operation: The London 2012 Olympic and Paralympic Games.* Press release, May 21, 2012.

https://news.npcc.police.uk/releases/police-service-delivers-resources-for-largest-ever-pre-planned-operation-the-london-2012-olympic-and-paralympic-games#:~:text=21%20May%202012-,Police%20service%20delivers%20resources%20for%20largest%20ever%20pre%2Dplanned%20operation,2012%20Olympic%20and%20Paralympic%20Games&text=A%20total%20of%2052%20individual,policing%20continues%20to%20be%20delivered

O'Brien, Chris. *Paris 2024 : French Government Approves Controversial AI Video Surveillance*. Forbes, March 31, 2023.

https://www.forbes.com/sites/chrisobrien/2023/03/31/paris-2024-french-government-approves-controversial-ai-video-surveillance/

- Paris 2024 Organising Committee. *Accreditation Terms and Conditions: Olympic Games Paris 2024*. Paris: Paris 2024 – Summer Olympic Games Organising Committee, 2024.

https://stillmed.olympics.com/media/Documents/Olympic-Games/Paris-2024/Accreditation/paris-2024-accreditation-terms-and-conditions.pdf

- Paris 2024 Organising Committee. *Opening Ceremony of the Paris 2024 Olympic Games: Media Guide, 26-07-24, 19:30*. Media guide. Paris: Paris 2024 Organising Committee for the Olympic and Paralympic Games, 2024.

file:///C:/Users/herau/Downloads/Media%20Guide%20-%20Opening%20ceremony%20(1).pdf

- Préfecture de Police (Paris). *Security Arrangements for the Opening Ceremony of the 2024 Olympic Games*. Press release. *2024.*

https://www.prefecturedepolice.interieur.gouv.fr/sites/default/files/Documents/press_release_security_arrangements_for_the_opening_ceremony_of_the_2024_og_0.pdf

- Prosegur Security. *Security Report: Olympic Games 2024 – Paris*. Intelligence and Foresight Unit, July 2024.

https://www.prosegur.us/dam/jcr:204a122c-f135-44f6-bb34-2a8fd765488e/July-2024_Olympic-Games-Paris_Final.pdf

- République française**.** *Loi n° 2018-202 relative à l'organisation des Jeux de 2024.* Journal officiel, 2018.

https://www.legifrance.gouv.fr/loda/id/JORFTEXT000036742943

- République française. *Loi n° 2023-380 relative à l'organisation des Jeux Olympiques et Paralympiques de 2024*. Paris: *Journal officiel de la République française*, 20 mai 2023.

https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047561974

- République française. *Paris 2024 Olympic and Paralympic Games stakeholders*. Government documentation. Published March 21, 2024; modified August 6, 2024.

https://www.info.gouv.fr/grand-dossier/paris-2024-olympic-and-paralympic-games/paris-2024-olympic-and-paralympic-games-stakeholders

- République française. *Plan A : ils l'ont fait !*. Ministry of the Interior. Published August 1, 2024; updated November 26, 2024.

https://www.interieur.gouv.fr/actualites/grands-dossiers/a-linterieur-des-jeux-olympiques-et-paralympiques-de-paris-2024/plan-a#:~:text=Policiers%2C%20gendarmes%2C%20sapeurs%2Dpompiers,soir%20mes%20plus%20sinc%C3%A8res%20remerciements.%20%C2%BB&text=Ce%2026%20juillet%2C%20les%20forces,pour%20acc%C3%A9der%20%C3%A0%20cette%20fonctionnalit%C3%A9.

- Reynaud, Florian, and Martin Untersinger. *Paris 2024 : la vidéosurveillance algorithmique à l'épreuve des Jeux olympiques*. Le Monde, July 23, 2024

https://www.lemonde.fr/pixels/article/2024/07/23/paris-2024-la-videosurveillance-algorithmique-a-l-epreuve-des-jeux-olympiques_6256418_4408996.html

- Samatas, Minas. *Surveillance in Athens 2004 and Beijing 2008: A Comparison of the Olympic Surveillance Modalities and Legacies in Two Different Olympic Host Regimes*. Urban Studies 48, no. 15 (November 2011): 3347–3366.

file:///C:/Users/herau/Downloads/SAMATASPAPERFORURBANSTUDIES_HI0001.pdf

- Samatas, Minas. *Security and Surveillance in the Athens 2004 Olympics: Some Lessons from a Troubled Story*. International Criminal Justice *Review* 17, no. 3 (September 2007): 220–238.

file:///C:/Users/herau/Downloads/SAMATAS-372813350359042146589703763 3_content_1.pdf

- Secrétariat général de la Défense et de la Sécurité nationale (SGDSN). *Summary of the Information Threat to the Paris 2024 Olympic and Paralympic Games*. Public Report, September 19, 2024.

https://www.sgdsn.gouv.fr/files/files/Publications/20240919_NP_SGDSN_VIGINUM_Summary%20information%20threat%20Paris2024Games_EN_0.pdf

- Spaaij, Ramon, and Andrew Zammit. *The Terrorism Threat to the 2024 Paris Olympics: Learning from the Past to Understand the Present*. Short Read. The Hague: International Centre for Counter-Terrorism, June 27, 2024.

https://icct.nl/publication/terrorism-threat-2024-paris-olympics-learning-past-understand-present

- Statewatch. *Security of the Spectacle: The EU's Guidelines for Security at Major Events*. Analysis No. 207. Brussels: Statewatch, December 2012. pp 36.

https://www.statewatch.org/media/documents/analyses/no-207-major-events-public-order.pdf

- Strom, Kevin J., and Joe Eyerman. *Interagency Coordination: Lessons Learned From the 2005 London Train Bombings.* NIJ Journal, no. 261 (July 2008): 28–32.

https://www.ojp.gov/pdffiles1/nij/224088.pdf

- The Olympic Museum. *The Modern Olympic Games*. Lausanne: International Olympic Committee – The Olympic Museum, 2013.

https://stillmed.olympic.org/media/Document%20Library/OlympicOrg/Documents/Document-Set-Teachers-The-Main-Olympic-Topics/The-Modern-Olympic-Games.pdf

- United Nations Office of Counterterrorism (UNOCT). *Securing the Legacy: Post-Games Debrief*. New York: UNOCT, March 5, 2025.

https://media.un.org/photo/en/asset/oun7/oun71088552

- United Nations Office of Counterterrorism. *Guide on the Security of Major Sporting Events: Promoting Sustainable Security and Legacies*. Global Programme on the Security of Major Sporting Events. New York: UNOCT, June 2021.

https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/211006_guide_on_security_major_sporting_events_web.pdf

- United Kingdom. Home Department. *Project CONTEST: The Government's Counter-Terrorism Strategy*. Government response to the Ninth Report from the Home Affairs Committee, Session 2008–09. Presented to Parliament by the Secretary of State for the Home Department. Command Paper Cm 7703. September 2009.

https://assets.publishing.service.gov.uk/media/5a7cbb48e5274a38e5756683/7703.pdf

- United Kingdom. Home Office. *London 2012 Olympic and Paralympic Safety and Security Strategy*. March 2011. Published by the Home Office.

https://assets.publishing.service.gov.uk/media/5a79575140f0b63d72fc4f5c/olympic-safety-security-strategy.pdf

- Vincent, John, John S. Hill, Andrew Billings, John Harris, and C. Dwayne Massey. *'We Are GREAT Britain': British Newspaper Narratives during the London 2012 Olympic Games*. International Review for the Sociology of Sport 53, no. 8 (2018): 895–915.

file:///C:/Users/herau/Downloads/vincent-et-al-2017-we-are-great-britain-british-newspaper-narratives-during-the-london-2012-olympic-games.pdf

- Voice of America. *Unprecedented Security Measures in Place Ahead of Olympics Opening Ceremony*. VOA News, August 12, 2004.

https://www.voanews.com/a/a-13-a-2004-08-12-12-1-66892312/261905.html

- West, Tim. *The Cyber Threat to Paris 2024 Olympics*. WithSecure Intelligence & Foresight Unit report, July 2024.

https://www.withsecure.com/content/dam/with-secure/en/resources-library/202407_WithSecure_Olympics_Threat_Report_ENG.pdf

- Wintics. *Cityvision: Détection d'anomalies pour les Jeux de Paris*. Paris: Wintics, 2024

https://wintics.com/a-propos/

- Yu, Hai, Francisco Klauser, and Ka-ming Chan**.** *Security and the Olympics: From Athens to Beijing.* The International Journal of the History of Sport 26, no. 3 (2009): 390–405.

file:///C:/Users/herau/Downloads/Governing_Security_at_the_2008_Beijing_Olympics.pdf

- Zatsepina, Nadezhda, and Martin Ludvigsen**.** *Algorithmic Policing and Democratic Risk at Mega-Events*. Information, Communication & Society 27, no. 9 (2024): 1501–1521.

file:///C:/Users/herau/Downloads/Algorithmic%20Olympics%20%20exploring%20the%20ethical%20and%20social%20implications%20of%20AI%20surveillance%20through%20the%20case%20of%20Paris%202024.pdf

- Zhou, Shuhua, Bin Shen, Cui Zhang, and Xin Zhong. *Creating a Competitive Identity: Public Diplomacy in the London Olympics and Media Portrayal.* Mass Communication and Society 16, no. 6 (November 2013): 869–887.

file:///C:/Users/herau/Downloads/Zhouetal.Olympics.pdf