



2020 Summer Olympics Event Assessment

Executive Summary

The 2020 Summer Olympic Games, also known as Tokyo 2020¹, are scheduled to be held from July 23, 2021, to August 8, 2021, in Tokyo, Japan. Originally scheduled to take place in 2020, the event was postponed as a result of the COVID-19 pandemic. Although Tokyo 2020 faces unique challenges, and its organizers' creativity and resiliency are being put to the test, no credible physical or cybersecurity-related threats associated with the upcoming Olympic events were identified as of the writing of this report. Nevertheless, concerns over the possible impact of ransomware attacks or nation-state activities on the Games persist.

Key Findings

- Despite consistent opposition against the Games by segments of the Japanese public and the declared state of emergency in Tokyo, the Japanese government and the International Olympic Committee have made it clear that Tokyo 2020 will be held on schedule, despite the recently declared state of emergency in Tokyo. Due to the pandemic, significant security precautions will be in place, including the barring of international spectators and potentially limiting domestic fans. Because of the fast-changing COVID-19 situation in the country, new restrictions are still likely.
- Overall, the threat of widespread unrest during the Tokyo 2020 events is low. ZeroFOX expects any potential upcoming demonstrations to be primarily concentrated in major population areas, particularly Tokyo, which could intensify in the weeks leading up to the opening ceremony on July 23, 2021. Despite increased media and security presence around key event sites, as well as the limiting of spectators during the Games, ZeroFOX expects the risk of sporadic, small-scale skirmishes between protesters and police to continue.
- ZeroFOX has identified no evidence of terrorist threats made against Tokyo 2020. The threat from organized domestic terrorist groups is low, as the Japanese government tightens anti-terrorism measures ahead of the Games. Similarly, while there are ongoing tensions in the region, the potential for a geopolitically-related incident to impact the Olympics remains extremely low.
- As with most large-scale sporting events, cybersecurity remains a concern for 2020 Summer Olympic Games. With Japan's over-dependence on digital infrastructure during the Olympics, there are potential risks if such systems are infiltrated. Furthermore, as

¹ Please note that despite being rescheduled for 2021, the event retains the *Tokyo 2020* name for marketing and branding purposes.

the threat of nation-state cyber attacks or ransomware attacks looms over Tokyo 2020, cybersecurity measures have become a must for Olympic organizers.

Event Preparedness

Security Measures

While most of the pre-Olympic focus has been concentrated on Japan's preparations for the ongoing COVID-19 pandemic, security preparations for the event venues, athletes, and spectators have been in development for several years.

While it is likely that the opening ceremonies for the Tokyo Olympics will be a TV-only event, the Tokyo Olympics organizing committee plans to set up security headquarters in each of the 48 event venues, including the Athletes' Village. As many as 18,000 private security guards will be deployed to help patrol the venues and surrounding neighborhoods. Unlike previous Olympics, organizers have stated that they are satisfied with recruitment levels and have enough private security guards to fully staff their security plan. As the number of spectators remains undecided, organizers have specified that flexibility is important until exact personnel numbers at venues are finalized.

Supplementing the security guards will be about 8,000 security cameras and 2,500 sensors, which will be installed in and around the sites and will monitor for apparent and hidden threats. Advances in artificial intelligence technology have improved the accuracy and effectiveness of facial recognition software, and the Tokyo Olympics hopes to use these advances to bolster its security posture. While the exact usage is undisclosed for security reasons, officials have announced plans to use this technology to potentially aid in identifying the faces of athletes, officials, and other personnel who have been authorized to enter restricted areas and to identify individuals who are in areas where they are not permitted to be.

Facial recognition is already commonly used in many areas throughout Japan. Passengers arriving at Terminal 3 of Narita International Airport can pass through customs by uploading photos of themselves to an app that is tied to the facial recognition system. Additionally, both Narita and Haneda airports in Tokyo are implementing a new facial recognition system called Face Express. The system will be used for all international flight boarding, regardless of airline, and will allow passengers to board flights without showing their tickets or passports.² The facial recognition procedure will automatically verify passengers boarding the flight and will be done without the need for staff to manually check airline tickets and passports at the gate. Face

²<https://www.securitymagazine.com/articles/94957-major-japan-airports-will-use-facial-recognition-for-international-flight-boarding>

Express requires passengers to register a photo of their face at check-in. Later, when boarding the plane, passengers will have their faces scanned by a camera instead of having to show their identification documents to airport staff. The new system is intended not only to expedite the process of boarding the plane but also to provide a contactless experience to limit the spread of COVID-19.

Along with private security personnel and facial recognition services, autonomous robots will also be patrolling the grounds to identify threats or hazards. These robots have 360-degree video cameras, as well as heat sensors and metal detectors. The robots are also equipped with extendable “arms” that allow them to check garbage cans and bags for suspicious items from a distance. The robots will communicate with people in multiple languages and send alerts to staffed monitoring stations.

Impact of COVID-19

While many prefectures in Japan have lifted full state of emergency guidelines imposed due to the COVID-19 pandemic and moved to a quasi state-of-emergency status, fears over the increase of cases in the country continue to grow, as only 26 percent of the population is fully vaccinated. On July 8, 2021, Prime Minister Yoshihide Suga will finalize any further emergency status guidelines. Thus far, dozens of municipalities in Japan have canceled their hosting arrangements because of virus concerns, and many of them have decided to use those facilities as vaccination sites.

Currently, Japan continues to enforce strict travel regulations that bar most new foreigners from entering the country. Foreign tourists and non-resident foreign business travelers remain prohibited from entry. The United States remains on Japan’s entry ban list due to its COVID-19 prevalence.³ Those individuals who are citizens or residents of Japan may enter the country but must adhere to pre- and post-travel restrictions. These restrictions include a 14-day quarantine and a negative COVID-19 PCR test within 72 hours of flight departure to the country.⁴

Concerns remain over the Olympics’ potential to become a superspreader event, given that roughly 100,000 athletes and others, not including spectators, will be entering the city for both the Olympic and Paralympic Games. As athletes from around the world start to arrive in Tokyo, several cases of athletes testing positive for COVID-19 have been reported upon arrival. Japan’s National Institute of Infectious Diseases and the head of a government COVID-19 advisory

³ <https://www.japan.travel/en/coronavirus/>

⁴ <https://jp.usembassy.gov/health-alert-us-embassy-tokyo-june-21-2021/>

On July 8, 2021 the Japanese government and Olympic Committee announced that spectators would be banned from entering Olympic venues in the Tokyo area. The cancellation of this aspect of the games follows increased concern about the spread of the Delta variant of COVID-19 in the Tokyo area. However, for venues outside of Tokyo, the Olympic committee is deferring to prefecture decisions about game attendance in person.⁶

Although demonstrators to date have largely focused their attention on the International Olympic Committee (IOC) and Japanese organizers, anti-government sentiment could become more evident in the weeks ahead. Prime Minister Yoshihide Suga's approval ratings have fallen to their lowest point since the start of his premiership in September 2020, hovering at about 30 percent. Suga has announced that he will not call for elections during the Olympics or Paralympics, which run until September 5, 2021. According to Japanese law, elections must be scheduled for October 21, 2021, at the latest, so the potential for anti-Olympics demonstrations

6

⁸<https://www.change.org/p/cancel-the-tokyo-olympics-to-protect-our-lives-stop-tokyo-olympic-cancel-the-tokyo-olympics>

to be co-opted by opposition parties and anti-government activists who see the Olympics as a roadblock to gaining control of the government is relatively high. Should the main opposition, the Constitutional Democratic Party of Japan, or another party successfully co-opt the anti-Olympic movement, more widespread protesting could occur.

ZeroFOX expects any potential upcoming demonstrations to be largely concentrated in major population areas, particularly Tokyo; these could intensify in the weeks leading up to the opening ceremony on July 23, 2021. Despite an increased media and security presence around stadiums and key event sites and the limiting of spectators during the games, ZeroFOX expects the risk of sporadic, small-scale skirmishes between protesters and police to continue.

Threat of Terrorism

ZeroFOX has identified no evidence of terrorist threats made against Tokyo 2020. Totemic targets of this nature with a global audience represent an attractive target for terrorist actors. Attacks against sporting events and stadia have occurred, including at the Atlanta Summer Olympic Games in 1996 and, more recently, at a soccer match in Paris in 2015. However, overseas spectators have been banned from attending the Games, almost certainly making the Tokyo Olympics a more difficult—and potentially less attractive—target for terrorist activity. Additionally, restricted numbers of domestic attendees have been permitted to attend the Games. While an attack could still generate significant media attention, the likelihood of high numbers of human casualties is greatly reduced. An attack is more likely to target densely populated areas of Tokyo rather than the Olympic Games specifically. Group protest activity is likely to be disruptive rather than life-endangering.

The threat from organized domestic terrorist groups is low. The group responsible for the 1995 Tokyo subway sarin attack that killed 13 and injured more than 5,000 people, Aum Shinrikyo (now operating under the name Aleph), reportedly continues to have a small following. However, the cult has been subjected to a sustained government crackdown; many individuals involved with the group have been arrested and convicted, and several members involved in the 1995 attack were executed in 2018. It is likely the Japanese government will tighten anti-terrorism measures against the group ahead of the Games.

While a number of overseas jihadist terrorist organizations, such as Al-Qaeda (AQ) and the Islamic State (IS), frequently encourage attacks against high-profile targets due to the shock and awe potential, they are unlikely to be able to mount an attack against the Tokyo Olympics directed by core leadership. A number of Japanese nationals are reported to have traveled to engage with the conflict in Syria, though it is not clear if any of these individuals have been allowed to return to Japan. Terrorist organization supporter groups and individuals may release “fanboy” media graphics or statements on private platforms threatening an attack. This trend is

common with major world events, including holidays, large sporting competitions, or other national celebrations. It is possible the reduction in spectator attendance could dissuade would-be attackers from targeting the Games.

The greatest terrorist threat to the Tokyo Olympics comes from low sophistication, lone-wolf attacks that are difficult to identify and mitigate due to the limited circle that has knowledge of such attack planning. An attack would most likely involve the use of easily accessible materials, such as bladed weapons, firearms, and rudimentary improvised explosive devices (IED), or vehicles as a weapon to target civilians in urban areas. Japan's most recent terror attack in 2019 involved an alleged Aum sympathizer who intentionally drove into pedestrians crowded into a narrow street in the Harajuku district of Tokyo, reportedly in retaliation for an execution.

Geopolitical Disruptions

While there are ongoing tensions in the region—which can largely be summarized as historical disputes, territorial conflicts, expanding influence, and rogue states—the potential for a geopolitically-related incident to impact the Olympics remains extremely low. Japan's foreign policy strategy places a significant emphasis on collaborating with other countries while pursuing its national interests, ensuring wider peace and prosperity in the international community, and being a peace-loving nation.⁹ This strategy in part helps maintain relationships with many of its immediate neighbors in the region. North Korea remains a wild card in the regional calculus; however, as the Olympics are an internationally sponsored event, it is unlikely that the regime will decide to act out. Furthermore, the Japanese government puts significant effort into maintaining positive diplomatic relationships with the United States and views the U.S. as one of its key strategic allies. The countries continue to share deep diplomatic, economic, and defense links. The United States also maintains a significant military presence in Japan and the wider region, which further acts as a deterrent to possible conflict escalations.

Cybersecurity Preparedness and Concerns

While ZeroFOX did not identify any planned cyber attacks against Olympic events or Tokyo 2020 sponsors, major international sporting events draw the interest of various threat actors. With the Games around the corner, Japan has demonstrated high-quality innovations and partnerships to increase protection during Tokyo 2020 and has made strides to improve its cybersecurity, particularly protecting its critical infrastructure. In 2020, Japan sought bilateral cooperation with the U.S. and other nations to operationalize its cybersecurity priorities, including a new agreement with the U.S. Department of Homeland Security to improve the

⁹ [hXXps://www\[.\]mofa.go\[.\]jp/files/100116875\[.\]pdf](https://www.mofa.go.jp/files/100116875.pdf)

sharing of cyber threat indicators between governments to improve its cyber readiness ahead of the 2020 Olympics in Tokyo.¹⁰

In addition, with Japan being a technology leader and the year-long postponement of this event to 2021, the country likely has gained an advantage by having the time to update its digital infrastructure, further bolstering confidence in the Games' cybersecurity. The country has established a Cyber Security Council tasked with coordinating efforts to defend and restore systems between different organizations and applying international law as needed during Tokyo 2020. The country's National Institute of Information and Communications Technology also surveyed over 200 million network-connected devices over the course of 2019, testing for unsafe username/password combinations primarily at public Internet access points and through Internet Service Providers.¹¹ Furthermore, the IOC also identified cybersecurity as a priority area and invested to provide the best cyber-secure environment for Tokyo 2020. However, the IOC noted that they would not be disclosing the specific details of their cybersecurity plan due to the nature of the topic.

Cyber threats to the Olympics, however, are not without precedent. The 2018 Winter Olympics in PyeongChang saw the highest level of attacks. Russian hackers carried out attacks on Olympic networks before the opening ceremony, which slowed down the entry of spectators and took Wi-Fi networks offline, affecting portions of the broadcast. Despite this thorough preparedness, any nation-state that is not aligned with Japan may see an opportunity to try to embarrass the Games host through a cyber attack. Japan has already faced multiple threats during the preparations for Tokyo 2020, most notably those allegedly stemming from Russia's Main Intelligence Directorate (GRU) unit's cyber reconnaissance activities. While Olympic organizers and government officials have disclosed few details on the specific tactics, techniques, and procedures (TTPs) used by Russia's military intelligence unit, Sandworm, to attack the Tokyo Olympics, its targets included the Games' organizers, logistics services, and sponsors. Authorities believe Sandworm intended to sabotage the Olympic Games, similar to the cyber attacks the unit carried out against the organizers of the 2018 Winter Olympic and Paralympic Games in PyeongChang, South Korea.¹² It is likely that nation-states will seek to conduct additional offensive operations throughout the duration of the Games. These offensive operations could take the form of data theft and leaks, misinformation, or disruption of systems involved in various sporting events.

¹⁰ <https://www.csis.org/events/cybersecurity-tokyo-2020>

¹¹ <https://www.cpomagazine.com/cyber-security/state-backed-cyber-attacks-expected-at-tokyo-2020-games/>

¹² <https://www.zdnet.com/article/uk-says-russia-was-preparing-cyber-attacks-against-the-tokyo-olympics/>

Furthermore, as the threat and pervasiveness of ransomware actors has increased dramatically over the last year, a ransomware attack on Tokyo 2020, the IOC, or a third-party vendor that could impact the Games is likely, as cyber criminals might see Olympics-related vendors as prime targets for extortion. In May 2021, the Japanese Olympic Committee revealed that it was hit by a ransomware attack in April 2021 as part of a breach in which hackers broke into a Japanese government contractor's data-sharing tool made by technology company Fujitsu. The Olympic vendors will have little tolerance for downtime during Tokyo 2020, which will make them key targets for attack by ransomware actors seeking a quick pay day.