



G7 SUMMIT

| Event Assessment |



Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 2:00 PM (EDT) on May 16, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Event Assessment - G7 Summit

Executive Summary

The ZeroFox Geopolitical Working Group has been tracking developments around the upcoming G7 Summit. The G7 Summit will be held in Hiroshima, Japan, from May 19 through May 21, 2023, and will gather leaders from Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States. Represented jointly by the President of the European Council and the President of the European Commission, the European Union (EU) participates in all discussions as a guest.

The G7 leaders are expected to discuss various topics on the economy and regional affairs, with the Russia-Ukraine conflict being at the center of the discussion. Stricter sanctions against Russia are expected to be discussed and potentially announced. There are rumors that the United States will propose a ban on all exports to Russia except for some medical and agricultural products. However, Japan and the EU have reportedly opposed such a proposal, stating that implementation of such a ban is unrealistic. Other expected geopolitical topics include restrictions on North Korea's nuclear program and missile testing and further calls for China to abstain from threats and use of force in Taiwan. Discussion on further trade and investments restrictions on China have also been mentioned, which includes a policy announcement calling on members to diversify their supply chains away from China.¹

Details

There have been concerns and public warnings about cyberattacks and physical security risks around the event based on the previous targeting of G7 summits. In the previous summits held in Japan, radical political groups targeted the event with explosives. Other summits held in Europe have experienced mass protests and terrorist attacks.

¹

[hXXps://www.bloomberg\[.\]com/news/articles/2023-05-13/g-7-finance-chiefs-unite-to-condemn-russia-and-counter-china](https://www.bloomberg.com/news/articles/2023-05-13/g-7-finance-chiefs-unite-to-condemn-russia-and-counter-china)



On June 8, 1979, during the fifth G7 Summit in Tokyo, a Japanese radical group called the Japan Revolutionary Communist League claimed responsibility for crashing a small, burning truck into the front gate of Japan's State Guest House.² On May 5, 1986, during the twelfth G7 meeting in Tokyo, the Japan Revolutionary Communist League was suspected of launching rockets over the State Guest House in Minato Ward, where a welcoming ceremony was being held.³ No injuries were reported in either incident.

Starting with the 2000 summit in Kyushu-Okinawa, Japan began a new tactic of holding the G7 at non-popular, isolated venues away from major cities. No significant security incidents were reported in 2000, at the 2008 summit in Hokkaido, or at the 2016 summit in Ise-Shima.

Analyst Commentary

Physical Security Threats

While Japan has historically been known as one of the safest countries in the world, with record lows in violent crime, the public's image of safety is changing due to attacks on politicians and the successful assassination of a former prime minister in 2022. Security measures in Tokyo and Hiroshima will be significantly increased during the summit. Airport, traffic, and sea travel delays are expected during this time due to closures of public travel routes and security checkpoints set up near summit-relevant locations. One focus of security attention will be the route from Hiroshima Airport to the main summit venue, a 55-kilometer journey that takes about 50 minutes by car.

The head of the Metropolitan Police Department said that, in addition to Hiroshima, police would exercise higher security measures in Tokyo throughout this period to protect embassies and government facilities.⁴ The Tokyo Metropolitan Police Department conducted several terrorist response drills to prepare for multiple scenarios of physical attacks targeting the event.⁵ During the summit, police will also work with the Japan Coast Guard to implement traffic and sea restrictions around central Hiroshima.⁶ From May 15, seafarers will be warned to avoid a zone within 300 meters of the island, and the Japan Coast Guard will intercept and inspect vessels that approach it.⁷

² [hXXps://japannews.yomiuri\[.\]co\[.\]jp/politics/g7-summit/20230502-107131/](https://japannews.yomiuri.co.jp/politics/g7-summit/20230502-107131/)

³

[hXXps://www.nytimes\[.\]com/1986/05/05/world/rockets-fired-at-palace-site-of-summit-welcome.htm](https://www.nytimes.com/1986/05/05/world/rockets-fired-at-palace-site-of-summit-welcome.html)

¹

⁴

[hXXps://english.kyodonews\[.\]net/news/2023/05/085eelbe0377-focus-security-in-spotlight-at-hiroshima-g-7-after-attacks-on-kishida-abe.html](https://english.kyodonews.net/news/2023/05/085eelbe0377-focus-security-in-spotlight-at-hiroshima-g-7-after-attacks-on-kishida-abe.html)

⁵ [hXXps://www.sankei\[.\]com/article/20230509-XAO4PUL32BK2XHY2SL2J35LKPY/](https://www.sankei.com/article/20230509-XAO4PUL32BK2XHY2SL2J35LKPY/)

⁶ [hXXps://www.japantimes\[.\]co\[.\]jp/news/2023/05/01/national/japan-security-g7-hiroshima/](https://www.japantimes.co.jp/news/2023/05/01/national/japan-security-g7-hiroshima/)

⁷ [hXXps://japannews.yomiuri\[.\]co\[.\]jp/politics/g7-summit/20230502-107216/](https://japannews.yomiuri.co.jp/politics/g7-summit/20230502-107216/)



The main venue for the G7 summit is the Grand Prince Hotel Hiroshima, known for hosting multiple international conferences. The hotel is located on the southeastern tip of Ujina, a small island in Hiroshima's Minami Ward waterfront area. The only road route to the island is via a bridge. Measures to prevent attacks on the venue from the ground will be aided by restricting access to Ujina and issuing passes to the island's residents, which number about 1,500.⁸

Advancements in drone technology have enabled scenarios in which remote drones can carry explosives to isolated locations, necessitating new vectors of vigilance. In March, the Hiroshima prefectural government established an ordinance penalizing the use of drones over areas within 2.5 kilometers (1.5 miles) of the island. The police will install drone detectors around the island and deploy security personnel equipped with devices that can jam drone signals.⁹

Leading up to the summit, multiple Japanese activist groups posted plans to protest against the G7 summit in Tokyo and Hiroshima. Typically most Japanese protests are peaceful and orderly, with rare unlawful disruptions ensuing from them. The following have been publicly announced:

- On May 18 and May 21, in Tokyo, a group called "Tokyo Action Committee Against the G7 Summit" will protest in the Shinjuku area. On May 18, the group will meet at 6:00 PM local time, and on May 21, they will be meeting at 2:00 PM local time.^{10 11} The meeting location will be the same on both days, with the group gathering outside of the shopping mall called Shinjuku ALTA located at 3-24-3 Shinjuku, Shinjuku-ku, Tokyo.
- In Hiroshima, anti-G7 protests will take place on May 19 and May 20. On May 19, a group called "the Local Demonstration Committee against the G7 Summit" will be meeting at Funairi First Park at 11:00 AM local time at 10 Funairi-cho, Naka-ku, Hiroshima-shi, Hiroshima.¹² On May 20, there will be two protests occurring in Hiroshima city. The first will be on May 20, starting at 11:00 AM local time and taking place outside of Hiroshima's Kinza Town Shopping District main entrance located at 1-6 Hondori, Naka-ku, Hiroshima-shi, Hiroshima.¹³ The second event will be on May 20, starting at 1:00 PM local time, and starting at Funairi First Park located at 10 Funairi-cho, Naka-ku, Hiroshima-shi, Hiroshima.¹⁴

⁸ [hXXps://japannews.yomiuri\[.\]co\[.\]jp/politics/g7-summit/20230502-107216/](https://japannews.yomiuri.co.jp/politics/g7-summit/20230502-107216/)

⁹ [hXXps://asianews\[.\]network/security-tightened-ahead-of-g7-summit-in-hiroshima/](https://asianews[.]network/security-tightened-ahead-of-g7-summit-in-hiroshima/)

¹⁰ [hXXp://antiwar2017\[.\]blog\[.\]jp/archives/39536840\[.\]html](https://antiwar2017[.]blog[.]jp/archives/39536840[.]html)

¹¹ [hXXps://twitter\[.\]com/mayumi3141/status/1657772511055220736](https://twitter[.]com/mayumi3141/status/1657772511055220736)

¹² [hXXp://www\[.\]labornetjp\[.\]org/EventItem/1681611858913matuzawa](https://www[.]labornetjp[.]org/EventItem/1681611858913matuzawa)

¹³ [hXXp://www\[.\]labornetjp\[.\]org/EventItem/1681552789227matuzawa](https://www[.]labornetjp[.]org/EventItem/1681552789227matuzawa)

¹⁴ [hXXp://www\[.\]labornetjp\[.\]org/EventItem/1681611953518matuzawa](https://www[.]labornetjp[.]org/EventItem/1681611953518matuzawa)



In the weeks leading up to the summit, there have been a string of unusual crimes in different areas of Japan:

April 15, 2023	April 25, 2023	April 30, 2023	May 8, 2023	May 10, 2023	May 15, 2023
A suspect was arrested for throwing an improvised explosive device near Prime Minister Fumio Kishida during his public visit to Wakayama City. Prime Minister Kishida was unharmed.	A suspicious item was reported in one of JR Hiroshima Station's bathrooms that caused police, the terrorist response team, and explosion specialist team to be brought in. The incident turned out to be a false alarm but locals had to take refuge, stores in the area were shut down, and trains were all delayed.	A woman was arrested for posting a threat on Twitter to release sarin gas in stations near Tokyo, purposely mimicking a well-known Japanese cult AUM Shinrikyo who attacked Tokyo subways with sarin gas in 1995.	A coffee can exploded at Nishiara Station in Tokyo, resulting in one woman being injured. The woman was doused with a liquid from the explosion that left her with burns on her face and body. Police arrested a suspect who caused the explosion through a chemical reaction using detergent. The arrested man, who holds Chinese nationality, told investigators that the explosion was not intentional, saying that he had placed a detergent from his workplace in the can to use at home.	Japan's special police squad was sent to inspect a suspicious item at Hiroshima Peace Park. This was deemed to be a false alarm.	Another false alarm occurred at Tenjingawa Station in Hiroshima, where Japan's special police squad was sent to inspect an additional suspicious item.

Recent Unusual Crime in Japan

Source: ZeroFox Intelligence

In addition, there have been other notable attacks associated with the G7 Summit historically:

2005	2007	2017	2021	2023
Britain Multiple terrorist attacks occurred in subways and buses in London around 600 kilometers from the summit venue, resulting in the loss of more than 50 lives.	Heiligendamm, Germany Anti-summit protestors rallied in the city of Rostock about 30 kilometers from the summit venue, and vandalized local shops.	Taormina, Italy Anti-summit protestors rallied against the event, with some clashing with local police.	Cornwall, England Some activists were arrested over an attempt to interfere with the event using smoke grenades.	Munich, Germany About 3,500 protesters have gathered in Munich ahead of the G7 Summit in the Bavarian Alps in Germany. At an earlier protest in the city, protesters wore oversized heads of the G7 leaders and demanded more global equality.

Previous Disruptive Activity Associated with the G7 Summit

Source: ZeroFox Intelligence

Cyber Threats

The number of cybercrimes uncovered by police in Japan hit a record high in 2022, rising to 12,369 cases—with notable growth in reports of ransomware attacks,



according to the National Police Agency. There were 230 reported cases of ransomware targeting in Japan—the highest number ever recorded in Japan’s history—with experts predicting cases will continue to increase. The daily average of suspicious internet access cases, including cyberattacks, also hit a record high of 7,707.9 per internet protocol address, the agency said.¹⁵

The number of cyberattacks, such as distributed denial of service (DDoS) attacks, against companies and government offices in Japan has been increasing since March 2023, ahead of the G7 meeting. However, according to sources, the DDoS attacks were mostly fixed quickly without causing significant disruptions. Japan’s National Center of Incident Readiness and Strategy for Cybersecurity has noted that a recent string of DDoS attacks targeting the West Japan Railway and Tokyo Electric Power Company Holdings, as well as the Osaka, Nara, Aichi, and Kumamoto prefectures’ websites, may have been a practice run for threat actors to prepare for larger-scale attacks ahead of or during the G7 summit.¹⁶

In addition, on May 8, 2023, an Anonymous-affiliated hacktivist group targeted the websites of Japan’s Justice Ministry in protest of the country’s refugee policy. In a statement on their Twitter account, hacktivists condemned “inhumane practices” and “warned” the Japanese government of further repercussions.¹⁷ A cyberattack during a large-scale event like the G7 Summit in Japan could provide an opportunity for various threat actors to draw attention to multiple grievances.

Cyber Concerns Related to the Russia-Ukraine Conflict

Since the Russia-Ukraine conflict will be among the central topics of discussion and decisions are likely to be made regarding the stance of the G7 countries, cyberattacks by pro-Russian hacktivists are possible and expected. Moreover, targeting various state and private organizations for their national government positions or actions in connection to the war in Ukraine has become a common occurrence and tactic among pro-Russian hacktivists and other threat actors.

For example, back in September 2022, pro-Russian hacktivist collective KillNet declared “war” on the Japanese government. According to the Russian-language video, which was subtitled in Japanese and posted by the group on its Telegram channel, “Russia is protecting its people from dangerous games conducted by European values and the United States. The Japanese are still waging an anti-Russian campaign. We are

¹⁵ [hXXps://www.japantimes\[.\]co\[.\]jp/news/2023/03/16/national/crime-legal/japan-cybercrime-rise/](https://www.japantimes.co.jp/news/2023/03/16/national/crime-legal/japan-cybercrime-rise/)

¹⁶

[hXXps://www.scmp\[.\]com/news/asia/east-asia/article/3218860/g7-ministers-focus-ai-risks-digital-infrastructure-pre-summit-meeting-japan](https://www.scmp.com/news/asia/east-asia/article/3218860/g7-ministers-focus-ai-risks-digital-infrastructure-pre-summit-meeting-japan)

¹⁷ [hXXps://twitter\[.\]com/Parrattarna/status/1655631501340422144](https://twitter.com/Parrattarna/status/1655631501340422144)



sending an official declaration of war on the entire Japanese government.”¹⁸ At the time, Japan’s Chief Cabinet Secretary Hirokazu Matsuno confirmed during a press conference that 23 websites operated by four ministries were inaccessible.²⁰ Matsuno then revealed that Japan was investigating the possibility that the access failures were caused by a DDoS attack launched by Killnet. Private Japanese companies have also reported that they have been potential targets of KillNet as well. According to major credit card company JCB, some of its websites were inaccessible, and they detected a DDoS attack caused by a large volume of access attempts.²¹ The Japanese social media service Mixi also reported a temporary service failure.

Some other recent examples of targeting foreign countries’ organizations for their pro-Ukraine positions include:

January 2023	February 2023	March 2023	April 2023
Pro-Russian hacktivist collective “KillNet” called on its supporters to target medical institutions in the United States and European countries over their support of Ukraine. While medical institutions are often spared from hacker attacks, this call to action was justified by KillNet as their response to the targeting of civilian infrastructure in the Donbass region. The group then posted expansive lists of potential targets in the Netherlands, the United States, Germany, the UK, Spain, Finland, Norway, and Poland.	Pro-Russian hacktivist collective “KillNet” carried out a series of distributed denial of service (DDoS) attacks against NATO-related websites causing temporary disruption to some of the military alliance’s public-facing websites. A NATO spokesperson confirmed that the alliance had briefly come under a cyber attack.	Pro-Russian hacktivists “Phoenix” targeted the Indian Health Ministry’s Health management system. The group justified the attack as a response to the recent reports that India allegedly will ensure no breach of Russia’s oil purchases as dictated by sanctions. According to the screenshots posted by the group, hackers managed to access the HMIS Portal, hospital, employee, and physician data.	Pro-Russian hacktivists “NoName057(16)” targeted Italian organizations, particularly in the banking industry, due to Italian prime minister Meloni’s statements that Italy would continue to support Ukraine. NoName057(16) previously targeted Italian organizations back in February when Meloni visited Ukraine in a surprise visit.

Recent Targeting of Organizations for Pro-Ukraine Position

Source: ZeroFox Intelligence

¹⁸ [hXXps://twitter\[.\]com/374News/status/1567490226242691073](https://twitter.com/374News/status/1567490226242691073)

¹⁹

[hXXps://www.japantimes\[.\]co\[.\]jp/news/2022/09/07/national/japan-government-cyberattack-russia/](https://www.japantimes.co.jp/news/2022/09/07/national/japan-government-cyberattack-russia/)

²⁰ [hXXps://www3.nhk.or\[.\]jp/news/html/20220907/k10013806911000.html](https://www3.nhk.or.jp/news/html/20220907/k10013806911000.html)

²¹ [hXXps://japannews.yomiuri\[.\]co\[.\]jp/society/general-news/20220914-58231/](https://japannews.yomiuri.co.jp/society/general-news/20220914-58231/)



Appendix: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.