# Winter Olympics 2026: Hacktivism Surges Ahead of Protests and Suspected Sabotage

By Intel 471

Published: 2026-04-01 · Archived: 2026-04-05 13:48:09 UTC

The 2026 Milan–Cortina Winter Olympics are a global stage — nearly three weeks of competition spread across Northern Italy, with thousands of athletes from 90 countries under the constant spotlight of international media. This visibility also makes the Games attractive to cyber threat actors, especially hacktivists who use the stage to amplify their ideological narrative through disruptive attacks. Indeed, since the opening of the games on Feb 6, Intel 471 have observed a surge in pro-Russia hacktivist activity targeting entities connected to the Olympics. As events continue to unfold, the security picture is also shaped by Russia linked advanced persistent threat (APT) group activity, and localized physical threats orchestrated by state-linked proxies. These large events also historically have triggered social activism with known or suspected links to state-backed hybrid warfare activity such as propaganda and disinformation operations.

In the lead up to the 2026 Winter Olympics, users on Telegram and X aligned with pro-Russian hacktivist campaigns highlighted previous efforts from Russia-linkedAPT groups that focused on reconnaissance and targeted attacks of the International Olympic Committee and adjacent organizations. This activity primarily occurred off the back of Russian athletes being banned from participating in the 2018 Winter Olympics as a result of the sports doping scandal and excluding Russia from the Olympics after its full-scale invasion of Ukraine in 2022. The 2016 to 2020 attacks consisted of state-backed spear-phishing campaigns and the destructive Olympic Destroyer malware, but activity targeting the Olympics that has been attributed to Russia since its invasion of Ukraine primarily has been aligned to low-level groups or hacktivists. This report is based on collections drawn from Intel 471's Cyber Geopolitical Intelligence, which monitors for geopolitical drivers of digital risk, and Adversary Intelligence, which tracks threat actors and groups using automated collection and on-the-ground human intelligence (HUMINT).

## Hacktivist claims about the 2026 Winter Olympics

Amid several ongoing geopolitical events in Europe, **NoName057(16)**, a dominant pro-Russian hacktivist, focused its cyclical distributed denial-of-service (DDoS) attacks against Italian entities located in the Olympics' host cities. Its initial claims behind the attacks spoke to Italy's ongoing support for Ukraine and propaganda commenting on the economic cost of hosting the Olympics. As the Olympic events kicked off February 6, 2026, the group narrowed its focus and claimed to have attacked three Olympic national teams. Several similar claims emerged, including:

- The **NoName057(16)** group taunted the head of Italy's National Cybersecurity Agency, questioning his ability to secure the country's national infrastructure.
- The **BD Anonymous** group announced an #Opitaly campaign and allegedly targeted websites of two Italian airports.

- The **Z-Pentest Alliance** and **Server Killers** groups claimed to attack an Italian human-machine interface (HMI) system and infrastructure in Italy, respectively.
- The **NoName057(16)** group allegedly conducted DDoS attacks against the Lithuanian, Polish and Spanish national Olympic committees, as well as a Cortina d'Ampezzo tourism website and Milan Malpensa Airport.

## Pro-Russia hacktivism alliances and Kremlin connections

The **Z-Pentest Alliance** and **Server Killers** group routinely are aligned with activity observed from **NoName057(16)**. Separately, **BD Anonymous** claimed its focus on Italy was due to the country not recognizing the independent Palestine state, although it is possible the group was influenced by **NoName057(16)**'s posts. The impact of **NoName057(16)**'s activity mostly was significant because the attacks were timed around the start of the Olympics. However, the group began claiming alleged attacks against Danish entities under its #OpDenmark tag February 9, 2026, suggesting it already moved on to a new area of focus.

In December, a Joint Cybersecurity Advisory and indictments assessed the Center for the Study and Network Monitoring of the Youth Environment (CISM) — established on behalf of the Kremlin — created the **NoName057(16)** group as a covert project within the organization. The documents claimed officials within CISM developed **NoName057(16)**'s proprietary DDoS tool DDoSia, paid for the group's network infrastructure, served as administrators on **NoName057(16)** Telegram channels and selected DDoS targets. The indictment also alleged **CyberArmyofRussia_Reborn** aka **Z-Pentest Alliance** was founded, funded and directed by the Main Directorate of the General Staff of the Armed Forces of the Russian Federation aka GRU.

## Beyond cyber: protests and suspected sabotage

Open-source reports have detailed protests and railway damage in Italy linked to the Olympic Games in recent days. The protests, which included violent demonstrations, seemingly were spurred by Italian citizens' discontentment with the economic situation in the country. The protestors specifically commented on cost-of-living issues in Italy and the long-term unsustainability of the Olympics. In situations where the protestors were armed and demonstrations turned violent against the police; several people were arrested. New security initiatives have been enacted in an attempt to keep unrest from spreading throughout the country while the Olympics are ongoing. Meanwhile, Italy's transport ministry is conducting an investigation into an arson attack on the Bologna-Venice railway line that disrupted transportation for several hours. It is currently being described as a suspected act of sabotage, as severed cables and explosive devices were identified in locations "nearby." No individuals or groups have claimed responsibility for the attack at the time of this report.

There are distinct parallels that can be drawn between protests and reported sabotage around the 2026 Milan-Cortina Winter Olympics and what was observed in the lead up to the 2024 Paris Summer Olympics. France deemed the reported sabotage targeting the Summer Olympics as acts of terrorism and the Italian prime minister has not minced her words regarding the violent activity from Italians. Some have also considered the additional arrest measures introduced after the physical altercations at the protests in Milan to be "repressive."

The combination of protests, transport disruption and amplified hacktivist activity creates a familiar challenge for host nations that can expect to face multiple pressure points at once competing for responder attention during a

peak-demand period.

## What's next in the cyber-geopolitical nexus?

The observed prevalence of hacktivism activity in the lead up to and start of the 2026 Winter Olympics is a continuation of expected cyber activity around highly publicized events. Italian authorities noted the activity and claimed to have stopped the attacks without any notable impact to the targeted entities. We cannot completely dismiss the possibility that Russian state-backed threat groups have conducted persistence attacks against entities involved in the 2026 Winter Olympics. However, this type of influence and the suggested need to defend Russia's image on the world stage likely are secondary or tertiary intelligence objectives for the Kremlin at present.

Without a dramatic reprioritization of strategic intelligence issues from Russia or other adversarial nations — such as China, North Korea or Iran — hacktivism likely will remain the most obvious and immediate threat encountered in high-profile global events. The diversity of state-aligned or adjacent cyber capabilities at these countries' disposal means it is no longer a requirement for more sophisticated threat groups to be deployed to carry out cyberattacks in such instances. Russia's offensive cyber groups will highly likely remain focused on the country's hybrid warfare efforts across Europe as it relates to targeted attacks against key strategic personnel and organizations dealing with policy decision making and military contributions to Ukraine in the ongoing war.

Separately, the social activity mirroring events in France around the 2024 Summer Olympics can be characterized as a statement on the current political, economic and social climate in some European countries. With expanding defense budgets and controversial international deals under consideration at the European Council, the cost of infrastructure to host the Olympics certainly will remain a contentious matter. Several ongoing geopolitical issues including the Russia-Ukraine war and Israel's actions in Gaza also have continued to fuel activism across Europe — notable in the sense that some established basis for civil activism creates an environment ripe for continued societal-led pressure against the government and state authorities. Because it is possible these collective issues culminated into a pattern of activity across the last two Olympics, protests can be expected to emerge at similar events in the near term.

The sabotage events noted in France and Italy echo several similar attacks against transportation infrastructure in Poland and the Netherlands, as well as arson attacks against businesses in Lithuania and the U.K. in recent years. These events largely have been suspected or directly attributed to Russia's expanding hybrid warfare activity across the continent. The attacks against Polish and Dutch rail lines seemingly align with initial reports about the sabotage attack in Italy, although Italian authorities have offered no suggestion that a foreign actor was involved. It is unlikely the Bologna-Venice rail attack can be attributed to Russia, although the potential for such an attack cannot be ruled out given the general heightened security risk across Europe at the time of this report.

## Quick wins for organizers, partners and agencies

- **Assume DDoS attempts and plan communications:** Pre-draft outage messaging, alternate domains/status pages, and escalation paths.
- **Harden identity and email:** Enable MFA everywhere possible and phishing-resistant MFA for high-risk roles.

- **Monitor brand abuse:** Fake Olympic ticketing, travel domains, social accounts will spike during the Games.
- **Monitor third parties:** Contractors, venues, and local suppliers often have weaker security postures.

---