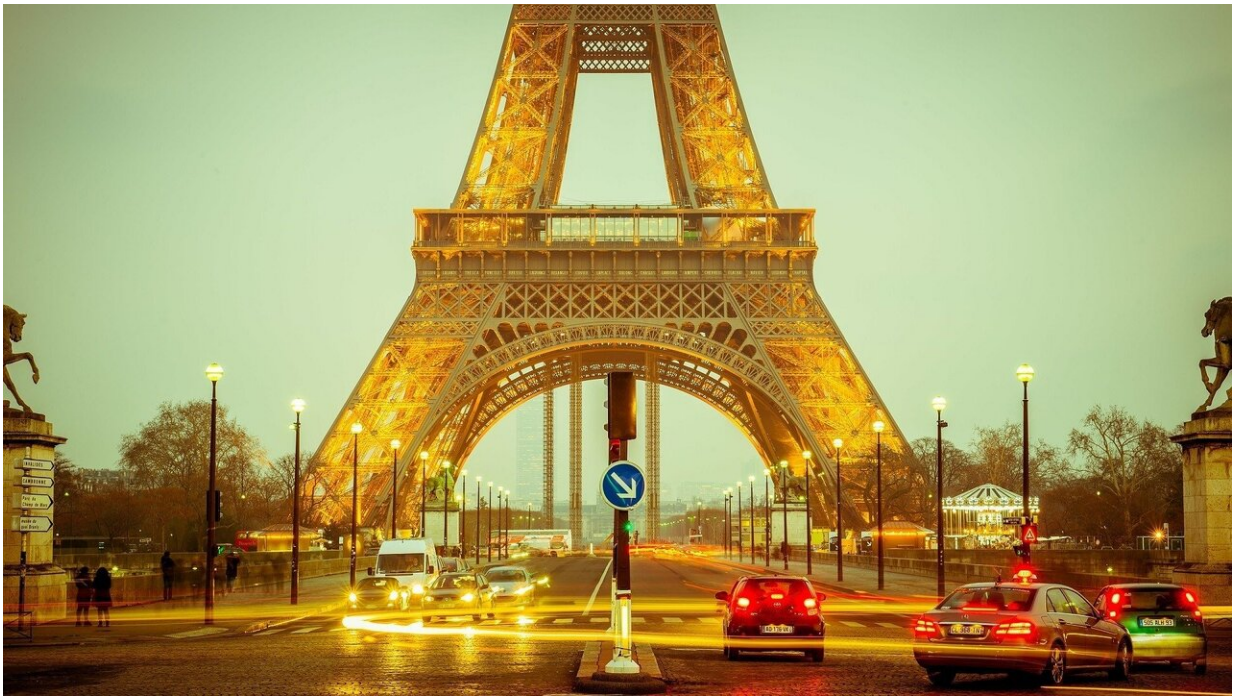
# Paris faces cyber battle to keep Games running and real

April 16 2024



Credit: Pixabay/CC0 Public Domain

The Paris Olympics are bracing themselves to fight off an unprecedented level of cyber attacks, for the first time augmented by artificial intelligence.

The kaleidescope of threats could come from criminal groups, states eager to undermine the Games, "hacktivists" with ideological ambitions,

gamblers or even athletes.

"There are so many moving pieces that the attack spectrum is quite large and it's a very serious security challenge," John Hultquist, an analyst at Mandiant Consulting, a cybersecurity consultancy owned by Google, told AFP.

"We are worried about everything from the broadcasters to the sponsors, transport infrastructures, logistics and support, competitions.

"Any kind of disruption is on the table."

Japanese telecom company NTT, which provided IT security for the pandemic-delayed Tokyo Olympics held in 2021, reported 450 million individual cyber attacks during the last edition of the Games, twice as many as during the 2012 London Olympics.

Fending off such attacks is primarily the responsibility of France's information systems security agency (Anssi) and interior ministry, with backup from the cyber defense arm of the defense ministry (Comcyber).

Vincent Strubel, the director general of Anssi, told AFP in March that his attitude to the threat was "neither nonchalance, nor panic".

"We've prepared hard. And we still have a few months to fine-tune," he added.

## 'Worst-case scenario'

"The worst-case scenario is that we end up drowning in attacks that are not very serious, and that we don't see a more dangerous attack coming, targeting a critical infrastructure," he added.

Cyber attacks are nothing new.

A risk management expert recalled in the research magazine Herodote the first cyber-attack on an Olympics, at Montreal in 1976, in the Stone Age of computing.

Those Games were hit by a 48-hour electrical disruption to information systems. Several events had to be postponed or moved.

International tensions multiply the risks. Russia, whose relations with the International Olympic Committee (IOC) are atrocious and whose athletes will not be able to compete under their national flag, has been suspected of several sports-related attacks already.

The IOC complained of Russian disinformation campaigns in November and March.

In 2019, Microsoft said that a Russian hacking group, Fancy Bears, had tried to attack the computer systems of several global anti-doping agencies.

Russian military intelligence services were blamed by the US for releasing the so-called "Olympic Destroyer" malware shortly before the opening ceremony of the 2018 Pyeongchang Winter Games in South Korea, from which Russian athletes were banned.

In early April, the Kremlin denounced President Emmanuel Macron's "unfounded" accusations that Moscow was disseminating information suggesting that Paris would not be ready for the Olympics.

"The point is geopolitical, it is to undermine trust and faith in a target and their ability to operate effectively," said Hultquist.

The Games will also be operating, for the first time, in the era of democratized and powerful artificial intelligence.

"AI will have a huge impact on us," said a senior French military official.

It will enable us to "shuffle data faster, and extract key events which will help us to attack our opponents". But they "have the same assets and, above all, I'm going to have a lot more adversaries."

"The resources are not up to the challenge of all the attacks we could suffer," he warned.

Attacks could target not only the operation of the venues, but also the local rail and metro systems, the Parisian electricity and water systems, telephone networks and media covering the Games.

"The highest risk is disruption of infrastructures and broadcast," said Hultquist. "You can literally have an effect on the game itself or on the ability of the world to see the Games.

"If nobody can see them, it is just as good as taking them down."

Attacks could also happen away from the Games with the spread of faked videos of the action.

We are entering "a new era where it will be easier to affect the integrity of sport thanks to AI", said Betsy Cooper, cybersecurity expert for the Aspen Institute in the U.S..

"Deep-fake videos could be used to distract from reality of a particular events."

## 'Paper back-up'

She also warned results could be altered in the venues: "Interference in the finish line camera, rigging a Hawk-Eye refereeing system, erasing times, scrambling scoreboards. The means of disruption are manifold."

She urged "compartmentalizing your data".

"Make sure if someone gets into one system, he does not enter all of them.

"You don't want the athletes to be connecting to the same network as the scoring system."

She recommended an old-fashioned solution.

"You need the paper back-up, you need the judges to write down the scores on a piece of paper somewhere that does not touch the system," she said.

"There are new vectors of threat this year that were not here for Tokyo and earlier Olympics."



Citation: Paris faces cyber battle to keep Games running and real (2024, April 16) retrieved 17 July 2024 from https://techxplore.com/news/2024-04-paris-cyber-games-real.html