France Blames Iran for Cyber Sabotage. What Happens Next?

11 NOVEMBER 2026

Bruna De Carvalho Santos Pineschi

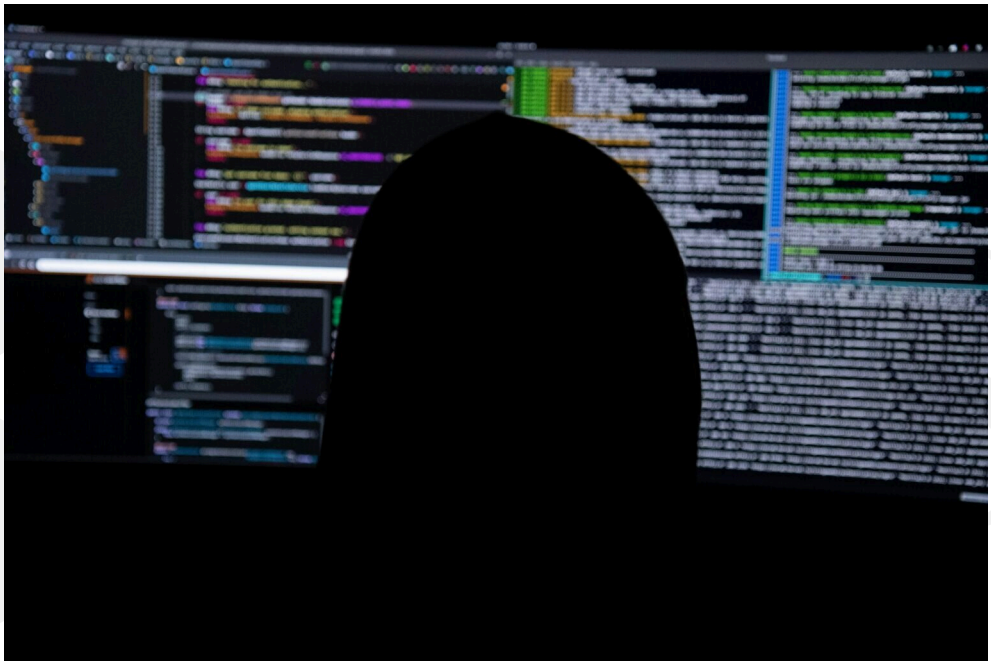


Photo by Kevin Horvat on Unsplash

On 9 November, France issued a statement attributing the October cyber-attacks against supermarket refrigeration systems to Shahid Kaveh, a unit affiliated with Iran's Revolutionary Guards. According to ANSSI, the attack affected approximately 700 commercial establishments, as well as the agri-food sector and small hydroelectric power plants, and reportedly caused at least 15 fires. The attribution adds new questions of cybersecurity and legal responsibility to the EPIS news published in October, when those responsible were still unknown.

In the statement, France asserted that the attacks violate international law and the UN norms on responsible state behavior in cyberspace, which the Islamic Republic of Iran had reportedly endorsed. And, on 10 November, the French government summoned the Iranian ambassador after announcing its intention to pressure the EU to impose sanctions. Meanwhile, the Paris Public Prosecutor's Office is also seeking individual

criminal accountability and has therefore requested international arrest warrants against members of Shahid Kaveh. Tehran, in turn, rejected the accusations, describing them as “unfounded”.

The problem is that merely attributing a cyberattack to a state does not automatically establish international responsibility. Under the ARSIWA, the conduct must also breach an international obligation, and the UN norms invoked by France are voluntary and not legally binding. However, this does not prevent France from responding.

Diplomatic measures and certain sanctions can be adopted regardless of whether a violation of international law has been established. But measures that would breach international obligations require stronger legal justification. By stating that it will adopt additional measures, public or not, France does not specify how it intends to respond and, consequently, which legal limits it must observe.

The October attacks exposed vulnerabilities in Europe’s networked infrastructure. But what happens when cyber-sabotage becomes a tool of conflict between nations? Is there any hope that international law can help to create justice?

EPIS