The Ramses Central Fire: Technical Failure or Advanced Cyberattack? A Security Analysis

حمزة حسن | July 8, 2025

This is an AI-generated English translation. The original text is in Arabic.

In recent days, Egypt witnessed a shocking incident represented by a massive fire at Ramses Central, which led to the suspension of many vital electronic services in the country, with widespread effects on communications and the internet. This incident was not merely a routine technical failure; it is considered a disaster by all standards that reflects the fragility of Egypt's digital infrastructure and reveals the extent of accumulated governmental failures over the past years.

In just one week, the coup regime led by Abdel Fattah el-Sisi faced a series of

shocks: repeated accidents on highways, frequent power outages, and finally, the central fire incident that exposed the fragility of devices and equipment, despite the massive spending over the past ten years. This situation has led some to question the possibility of hidden hands trying to strike and weaken the regime amid increasing internal and external tensions.

But could this fire be the result of a sophisticated cyberattack? The reality is that technology today allows for multiple scenarios, where advanced cyberattacks can lead to serious physical damage, not just the disruption of data or services.

How can cyberattacks cause fires?

There is a rare and advanced type of cyberattack that exploits vulnerabilities in devices and systems to control their operation in ways that lead to physical damage, such as:

- **Disabling the cooling system:** An attacker may stop or disable the cooling system of devices, leading to excessive overheating and consequently burning them.

- **Overloading the processor:** Commands can be sent to make the processor operate at maximum capacity for an extended period, raising its temperature to dangerous levels.

- **Electromagnetic attacks (EM Attacks):** Specialized devices are used to send electromagnetic signals that affect the electrical circuits within devices, causing damage or ignition.

Executing these attacks remotely requires vulnerabilities in the security system or an unsecured network, while attacks relying on direct electrical impact require physical proximity or advanced equipment.

Countries capable of executing such attacks include the United States, Russia, China, Israel, and other advanced nations in the field of cybersecurity.

What does this mean for Egypt?

The Ramses Central fire incident is not just a technical failure; it is an indicator of a vital infrastructure that is vulnerable to increasing risks in a world where cyberattacks are becoming more complex and dangerous due to poor financial management in Egypt and rampant corruption over the past ten years. Nevertheless, questions remain about the coup regime's readiness to confront these challenges, especially amid growing doubts about the existence of deliberate attacks aimed at destabilizing political and economic stability.

Ultimately, what Egypt has recently experienced in repeated incidents places the country before a real test of its ability to protect its electronic infrastructure, which has become a fundamental pillar of daily and economic life.