The European Union's Cyber War Challenge

By

Musa Khan Jalalzai

Hostile states actors are knocking on every closed door in Europe in an effort to disrupt normal management of societies and their governments. State institutions, including intelligence agencies, cybersecurity organizations, and policing agencies are exhausted in their efforts at pushing back against non-native and unknown forces.

Those European intelligence agencies tasked with countering malicious cyber actors are simply unprepared for the fight they face. Disinformation campaigns waged by the Chinese, North Koreans, and Russians are also plaguing Europe. When Russia first began such efforts to shape election outcomes about a decade ago, their rather low-cost efforts were successful enough to encourage further disinformation efforts.

French efforts to sound the alarm about disinformation in Europe and Africa were largely unheeded and is now bearing fruit for China and Russia as several African nations are turning against the West and toward these autocracies. The cyber four of China, Iran, North Korea, and Russia, through their security institutions, targeted the UK and French institutions, financial markets, and security infrastructure at home and their prestige abroad.

In response to the exponential growth of cyberattacks, in April 2023, new regulations were passed in France to secure the computer networks of state institutions. The French government also recognized the importance of international security cooperation in combating cyber terrorism.

When the French rail network was vandalized in July 2024 the French Interior Minister warned of the possible involvement of foreign cyber warriors. Saboteurs had already carried out attacks against fiber-optic cables and other infrastructure. For months, French intelligence was on its heels as consecutive attacks on the country's critical infrastructure occurred. Russian and other European nationals were arrested for varying destabilization attacks. French intelligence and police also launched an operation to find cyber sleeper cells.

The Olympics began as thousands of police and military personnel were operating across the country in an effort to prevent future terror attacks of any kind. If the cyberattacks on France prior to the Olympics are an indicator of a looming threat, France has its work cut out for it.

Cyber threats are more than just hackers exploiting the internet. On July 26, 2024, terrorists damaged lineside communication cables on three of the most important *ligne a vitesse* radiating from Paris. These attacks disabled signal technology at key junctions including in *LGV Nord* at Croisilles—connecting Paris with Lille. Eurostar rail networks were also disrupted ahead of the Olympics. Thus, damage to communication networks can take a physical form.

China is now engaged in open hybrid warfare against the West—more broadly. Policymakers, parliamentarians, and intelligence officials in the UK and France sometimes advocate for reforms to address these challenges, but little happens. The lack of cyber expertise within European intelligence agencies leads to numerous domestic security challenges. The French government, for example, was exasperated with the sabotage campaign that took place.

France accused Russia of cyberattacks during the election earlier this year—all to disrupt the country's democracy. Authorities asserted that the Russian Federal Security Service was behind sustained attempts against the French institutions.

The UK took measures in response to cyber threats from China, demonstrating a proactive stance, but British efforts are not widely understood and accepted. Recent cyberattacks on the UK's National Health Service and the Ministry of Defense highlight significant challenges faced by the Government Communications Headquarters (GCHQ) in countering hybrid warfare tactics from state actors like China and Russia.

These attacks illustrated vulnerabilities in the UK's cybersecurity infrastructure and raised concerns about the effectiveness of GCHQ's strategies in mitigating threats posed by advanced persistent threat (APT) groups.

In July 2024, cyberattacks on the NHS disrupted critical healthcare services, compromised patient data, and operational capabilities. Attacks on Ministry of Defense infrastructure jeopardized national security by leaking sensitive information and undermined military readiness.

The presence of foreign spies within UK state institutions suggests these networks have successfully penetrated high-security environments, posing substantial risks to national security. The presence of a strong Russian security and intelligence infrastructure in Eastern Europe, and its reluctance to accept Western security-sector reforms is a threat to internal and external security for the region.

In Eastern Europe, reshaping intelligence and police services is part of the consolidation of democracy. In the Czech Republic, Bulgaria, Hungary, Poland, and Romania, intelligence agencies are experiencing a cultural hangover from a bygone era. In these countries, the process of bringing intelligence services into a Western way of operating is progressing slowly.

The war in Ukraine is also leaving a deep impact. European intelligence service strategies, operations, and collection processes in and outside their sphere of influence. They never realized how to introduce the reforms required to prevent Russian success. The Danish, for example, produced the *PET Report*, which uncovered espionage networks in Denmark. The *PET Report* has noted several cases that illustrated how a number of foreign states were actively carrying out intelligence activities against Denmark using cyber and other means.

In short, Europe is facing a challenging future when it comes to the malicious cyber activities of China, Iran, North Korea, and Russia. European intelligence services are unprepared for the adversary they face. The challenge is growing. The time is now for Europe to respond.

Musa Khan Jalalzai is an author, journalist, and member of Research Institute for European and American Studies, Director of Law Enforcement and Intelligence Analysis Centre London, and Fellow of Islamic Theology of Counter Terrorism. The views expressed are his own.