Poland's Escalating Cyber Conflict with Russian-Backed Threat Actors

September 15, 2025

Poland has emerged as the primary battlefield in Europe's silent, ongoing cyber war. Due to its pivotal role as a military and logistical hub supporting Ukraine, the nation finds itself in the crosshairs of relentless digital campaigns orchestrated by Russian-backed threat actors. For years, this conflict has played out through espionage, disinformation, and disruptive attacks on government and energy networks.

However, the conflict has recently entered a far more dangerous phase. In a severe escalation, cyber attackers have moved beyond targeting data and disruptions to directly assault the fundamental infrastructure of daily life. The most alarming incidents involve successful breaches of hospital systems, which forced operational shutdowns and the theft of sensitive medical data, and a near-catastrophic attack on the water supply of a major city, where hackers were stopped only at the last moment from shutting off water to residents.

The most severe escalation in Poland's cyber conflict occurred recently, when Russian-backed hackers successfully targeted the core of the nation's civilian infrastructure. In a coordinated campaign, attacks breached several hospitals, forcing operational suspensions and resulting in the theft of sensitive medical data. Most critically, the same threat actors infiltrated the IT network of a water supply facility in a major Polish city. The attackers were stopped by authorities moments before they could shut off the water taps, narrowly averting a widespread humanitarian disaster. This incident represents a direct attempt to sabotage essential life-sustaining systems and has triggered a major policy and budgetary response from the Polish government.

The Broader Cyber Conflict: Context and Escalation

This attack on critical infrastructure is not an isolated event but the peak of a sustained "cyber cold war," as declared by Digital Affairs Minister Krzysztof Gawkowski. Poland is the primary target for Russian-backed cyber aggression within the European Union, a status confirmed by its position as the world's most targeted country for politically motivated "hacktivist" attacks. Pro-Russian groups execute a coordinated campaign, launching between 20 to 50 daily attempts to damage Polish critical infrastructure, with targets spanning government institutions, the energy sector, and military assets.

Pattern of Hostile Activity and Past Incidents

The threat landscape is diverse and persistently hostile. Prior to the recent crisis, Polish cybersecurity services have consistently dealt with major incidents, including:

* Space Agency Breach: The IT infrastructure of the Polish Space Agency (POLSA) was compromised, requiring the network to be disconnected to secure data.

* Athlete Data Leak: A sophisticated Russian-Belarusian linked sabotage group breached the national anti-doping agency (POLADA), leaking tens of thousands of confidential athlete files after extorting government agencies.

* DDoS Campaigns: Poland has been a prime target for disruptive DDoS attacks, often facilitated by international "DDoS-for-hire" services targeting schools, government services, and gaming platforms.

Poland's Strategic Response and Fortification

In response to this escalating threat, Poland has adopted a robust and multi-faceted defense strategy:

* Record Investment: In direct response to the attacks on hospitals and water systems, the government announced a record €1 billion cybersecurity budget, a massive increase from the previous year. This includes a specific €80 million allocation to immediately fortify water management systems.

* Proactive Operations: Poland does not only play defense. Its Central Cybercrime Bureau led an international operation to arrest administrators of a major DDoS-for-hire empire, disrupting a key source of cyberattacks.

* Legal & Systemic Strengthening: The government is amending the National Cyber Security System law and has achieved a rare cross-party political consensus on the need for enhanced digital defenses. Polish services successfully thwart approximately 99% of the daily attacks they face.

Poland finds itself on the frontline of a hybrid conflict, facing relentless cyber campaigns aimed at destabilization and sabotage. The recent direct attacks on hospitals and water supplies mark a dangerous new chapter, moving beyond espionage and disruption to direct threats against public safety. The Polish government is responding with unprecedented financial investment and strategic coordination, solidifying its defenses to protect its critical infrastructure and national security.