

Tallinn, 18 June 2026

No 3-8/26-101/4

Dear Colleague,

I am writing to draw your attention to key findings from the recently published Estonian Internal Security Service (Kaitsepolitseiamet, KAPO) Annual Review 2025–2026, which offers valuable insight into the evolving security landscape affecting the European Union.

According to the report, the principal security threat to Estonia—and by extension to the EU—continues to originate from the Russian Federation. KAPO highlights that Russia’s activities are not limited to conventional military aggression but increasingly rely on hybrid methods, including coordinated influence operations, cyberattacks, intelligence activities, and the exploitation of social media platforms to undermine democratic institutions and societal cohesion. These efforts are amplified by digital technologies and artificial intelligence, making them more scalable and harder to detect.

The report further underlines a growing trend in the use of loosely connected individuals, recruited through online channels, to carry out hostile actions such as information gathering or acts of sabotage. This “low-cost, high-impact” model complicates attribution and increases the vulnerability of open societies.

Cybersecurity is identified as a critical area of concern. State-linked actors increasingly target official email systems and cloud services, relying on stolen credentials and phishing campaigns to gain access to sensitive information. These activities can directly affect EU cooperation, particularly in areas related to support for Ukraine and the protection of critical infrastructure.

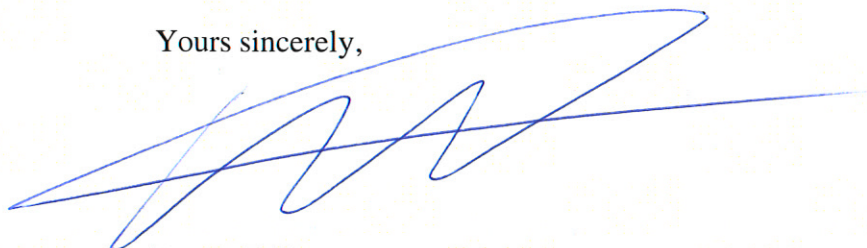
In addition, KAPO highlights concerns regarding the role of institutions connected to the Russian state, including the Russian Orthodox Church. The report notes that structures affiliated with the Moscow Patriarchate have, in certain cases, been used to support or justify Russian state interests and foreign policy objectives, including the war in Ukraine. Such activities may contribute to influence operations and pose risks to public order and security within EU member states.

At the same time, KAPO notes the expansion of long-term influence activities by the People’s Republic of China, particularly through cultural, academic, and economic engagement designed to shape perceptions and policy environments within Europe.

In light of these findings, I respectfully recommend strengthening EU-wide coordination in countering hybrid threats, enhancing cyber defence capabilities, improving enforcement of sanctions regimes, and increasing transparency regarding foreign influence operations. Equally important is the need to invest in societal resilience, including media literacy and public awareness.

The KAPO Annual Review clearly demonstrates that Europe's security challenges are interconnected and persistent. A unified and proactive response is essential to safeguard the integrity of our democratic systems.

Yours sincerely,



Peeter Tali
Chairman
European Union Affairs Committee of the Riigikogu
Riigikogu