

A GRU military unit launched cyberattacks against Estonian authorities

 prokuratuur.ee/en/news/gru-military-unit-launched-cyberattacks-against-estonian-authorities



Breadcrumb

- 1.
2. [News](#)
3. [A GRU military unit launched cyberattacks against Estonian authorities](#)

05.09.2024 | 20:06

Share

The National Criminal Police conducted criminal proceedings under the direction of the Office of the Prosecutor General, and found that the same unit launched attacks against Estonian state authorities in 2020. The criminal proceedings helped to identify three GRU officers suspected of the attacks: Yuri Denisov, Nikolay Korchagin and Vitali Shevchenko.

“Based on the suspicion, all three were serving in GRU’s military unit 29155 at the time of the attacks. We identified the first suspect and leads at the early stages of the investigation, and this allowed us to prevent more extensive damage and block its spread in cooperation with other agencies,” said Ago Ambur, head of the Cybercrime Bureau.

The Office of the Prosecutor General applied to the Harju District Court to commit the three suspects connected to the attacks on Estonia in custody. The Harju District Court granted the application and issued orders on committing the persons in custody *in absentia*.

State Prosecutor Vahur Verte says that the three men have been declared international fugitives from justice under the orders committing them in custody. “Although the suspects are currently in Russia as far as we know, international searches and orders on committing them in custody mean that they are in real danger of being detained by a state and surrendered to Estonia in order to answer charges in court when they travel outside Russia,” says State Prosecutor Verte.

Estonian Internal Security Service and international partners shared mutually important information that complemented the details available to Estonia and its partners during the different stages of investigation within the framework of joint operation Toy Soldier. Especially information concerning the cyber unit that launched the attacks. Charges have been brought against two of the suspects identified in Estonia, Denisov and Korchagin, in FBI proceedings as well. The US is offering a reward of 10 million dollars for the suspects.

GRU’s military unit 29155 is responsible for a coup d’etat attempt, sabotage and diversion operations and murder attempts in Europe. The purpose of the Russian Federation is to demolish and reshape European security architecture and rule-based world order, and revert to politics based on the concept of spheres of influence. This is why the cyber capability acquired by GRU’s military unit is a threat to Estonia’s national security.

“Cyber operations that allow sabotaging, gathering intelligence or conducting information operations are a significant part of hybrid warfare based on the Russian Federation’s military doctrine. We also defend Estonia’s national security in cyberspace, and in addition to spies in the flesh, we unmask cyberspies,” says Margo Palloson, Director General of the Estonian Internal Security Service.

29155 continues to act against Estonia’s state networks and other states. Thanks to the National Criminal Police, Estonian Internal Security Service and the Estonian Information System Authority’s (CERT-EE) cooperation in guaranteeing cybersecurity we have succeeded in identifying and blocking the attacks.

Consistent work with detecting and remedying both human and system dependent vulnerabilities protects the state's cybersecurity. This includes modernising systems, removing security vulnerabilities on a routine basis, segregating networks and implementing multi-level authentication.

Estonia names Russia's military intelligence in a first-ever attribution of cyberattacks: <https://vm.ee/en/news/estonia-names-russias-military-intelligence-first-ever-attribution-cyberattacks>

Statement of the United States of America: <https://www.justice.gov/opa/pr/five-russian-gru-officers-and-one-civilian-charged-conspiring-hack-ukrainian-government>

Further questions

[(#)]