

MASS DDOS CYBERATTACKS ON ESTONIA AFTER BRONZE SOLDIER RELOCATION

From late April to mid-May 2007, during the dispute over relocating the Soviet war memorial in Tallinn, Estonian government, media and banking websites were hit by large-scale distributed denial-of-service attacks. Estonia's foreign minister said part of the traffic came from Russian state IP addresses; Russia denied involvement and refused investigative cooperation. The only conviction was of an Estonian resident; no Russian state actor has been charged.

UKRAINE EVIDENCE HUB

BEYOND UKRAINE

AS OF 15 OCT 2026

DEGREE OF PROOF

OFFICIAL ATTRIBUTION

A government, a prosecutor, the EU, NATO or a UN body has formally named Russia, its services or its state-backed forces. This is a position of that authority, not a verdict.

WHO ESTABLISHED IT

Estonian Foreign Minister Urmas Paet, press conference 1 May 2007: Estonia had proof attacks came from 'IP addresses of governmental authorities of Russia' (reported speech); later accused the Kremlin of direct involvement. Defence Minister Jaak Aaviksoo later said he could not state for certain the attacks were managed by the Kremlin.

LATEST

Single conviction: Tallinn student Dmitri Galushkevich fined 17,500 kroons on 24 Jan 2008 for attacking the Reform Party website. A Nashi activist claimed involvement in 2009. The attacks led to the NATO CCDCOE being established in Tallinn (May 2008).

SOURCES

- B

Estonian Foreign Minister Urmas Paet press conference, as reported by Delfi (via eesti.ca) · 2007-05-02

<https://www.eesti.ca/paet-russia-attacks-estonia-and-the-european-union-delfi/article16198>
- C

Christian Science Monitor: Estonia accuses Russia of 'cyberattack' · 2007-05-17

<https://csmonitor.com/2007/0517/p99s01-duts.html>
- C

Baltic Times: Kremlin denies involvement in cyber attacks on Estonia · 2007-05

<https://www.baltictimes.com/news/articles/17908>
- C

InformationWeek: Estonian Hacker Fined For Cyber Attack · 2008-01

<https://www.informationweek.com/cyber-resilience/estonian-hacker-fined-for-cyber-attack>

WHAT WE ASK
OF MEMBER STATES

- Attribute jointly and raise it in the UN Open-ended Working Group on ICT security.
- Use the EU cyber sanctions regime against the units responsible.
- Share indicators and support the resilience of critical infrastructure.

Status follows four degrees of proof: court finding · official attribution · charged · suspected (suspected cases are listed only on the live page). Tier A = courts, UN bodies, international organisations · B = governments, prosecutors · C = media and investigators. Corrections: evidence@ukraine-evidence.org

