

RUSSIA'S STATE-LINKED CYBER THREAT ACTORS

Where the Kremlin's cyberattack “cells” actually come from

Most Russian state-linked cyberattack groups trace back to three intelligence and military organizations, each with a distinct role and headquarters in Moscow.



GRU

Military Intelligence — the most aggressive of the three

Cyber units based at GRU headquarters in Moscow; tied to destructive attacks such as NotPetya. Unit 26165 (APT28 / Fancy Bear) — active since at least 2004; linked to election-interference operations. Unit 74455 (Sandworm / Voodoo Bear / Telebots) — responsible for NotPetya and the 2016 U.S. election data leak; six officers carry a \$10M U.S. State Department reward. Unit 54777 (72nd Special Service Center) — disinformation and psychological operations, not intrusion.

FSB

Domestic Security Service — KGB's successor

Hybrid role bridging state operations and the criminal hacking underground. Known as APT29 / Cozy Bear / “The Dukes” — operates through two sub-centers. Center 16 — more aggressive; phishing and interception. Center 18 — espionage and information collection.

SVR

Foreign Intelligence Service — the “scalpel”

Focused on stealth, long-term espionage, and persistent access rather than destructive attacks. Prioritizes remaining undetected inside target networks for extended periods over causing visible damage.

Beyond the formal units: Russia also draws on a wider pool of “patriotic hackers” and criminal groups that it tacitly tolerates or actively recruits. Cybercriminals are reportedly sometimes offered dropped charges in exchange for working with intelligence services, provided they avoid targeting Russian entities.

Geography: these groups are Moscow-headquartered, following their parent agencies — though some earlier operations (e.g., against Georgia in 2008) used front infrastructure and youth-group intermediaries physically located near GRU headquarters to obscure state involvement.