

14 August 2026

Contact: alex.cyber@protonmail.com



Russia: cybercrime and punishment (2,490+ convictions in Russia since 2014)

Alexander Seger, 14 August 2026

Anyone investigating cybercrime knows the frustration: Russia is the main source of cybercrime, yet offenders operating from there remain largely out of reach. Investigations get shelved. Prosecution gives way to "disruption" – often with limited and temporary impact.

But do criminals in Russia really get away with it? And what happens to those wanted by foreign authorities?

New research by [Oleg O.](#) – "Crime and Punishment in the Russian-Speaking Cybercriminal Underground" – puts hard numbers on these questions (link in the comments):

- ◆ Cybercriminals DO get convicted in Russia: 2,490 convictions between 2014 and 2025. That is cybercrime in the narrow sense – not counting broader charges like aggravated fraud that cannot be isolated in the statistics.
- ◆ The "untouchable" myth is not abolished but narrowed. Impunity is real for parts of Russia's cybercriminal ecosystem, but it is neither uniform nor guaranteed. As the study puts it, it is "politically granted, conditionally maintained, and always revocable."
- ◆ Between 2000 and 2025, foreign (mostly US and European) authorities publicly announced 387 indictments or sanctions against suspected cybercriminals in the former Soviet space. 265 targeted suspects in Russia – initially for financial cybercrime, and from 2016 onwards also for state-linked activity (GRU officers, hybrid cases like Evil Corp).
- ◆ Of those 265 Russian suspects, 82 (31%) were eventually arrested. But almost none of these arrests happened in Russia. About 70 were captured abroad and then extradited or tried in a third country.

The pattern is clear: Russian cybercriminals wanted by foreign authorities are typically protected – as long as they stay in Russia. The moment they travel abroad, be it for leisure, relocation, or operational needs, they are at risk.

Compare that with other former Soviet states, which arrest their nationals on foreign requests far more often, even though some of these states cannot extradite their own citizens: 69% of Ukrainian suspects wanted by foreign authorities have been arrested.

My takeaway: international criminal justice action against cybercriminals in Russia makes sense – and makes life genuinely difficult for them.

Or as the study concludes: Inside Russia, they depend on the authorities for immunity and protection. But that protection is closer to confinement than freedom: It “rests on the goodwill of a state that owes them nothing, and the longer they depend on that goodwill, the more they belong to the system that protects them”.

And when they do travel? Many attractive holiday destinations happen to be parties to the Budapest Convention on Cybercrime. 🌴

Link to study: <https://www.cybercrimediaries.com/crime-and-punishment-in-the-russian-speaking-cybercriminal-underground>

www.alexnotes.net