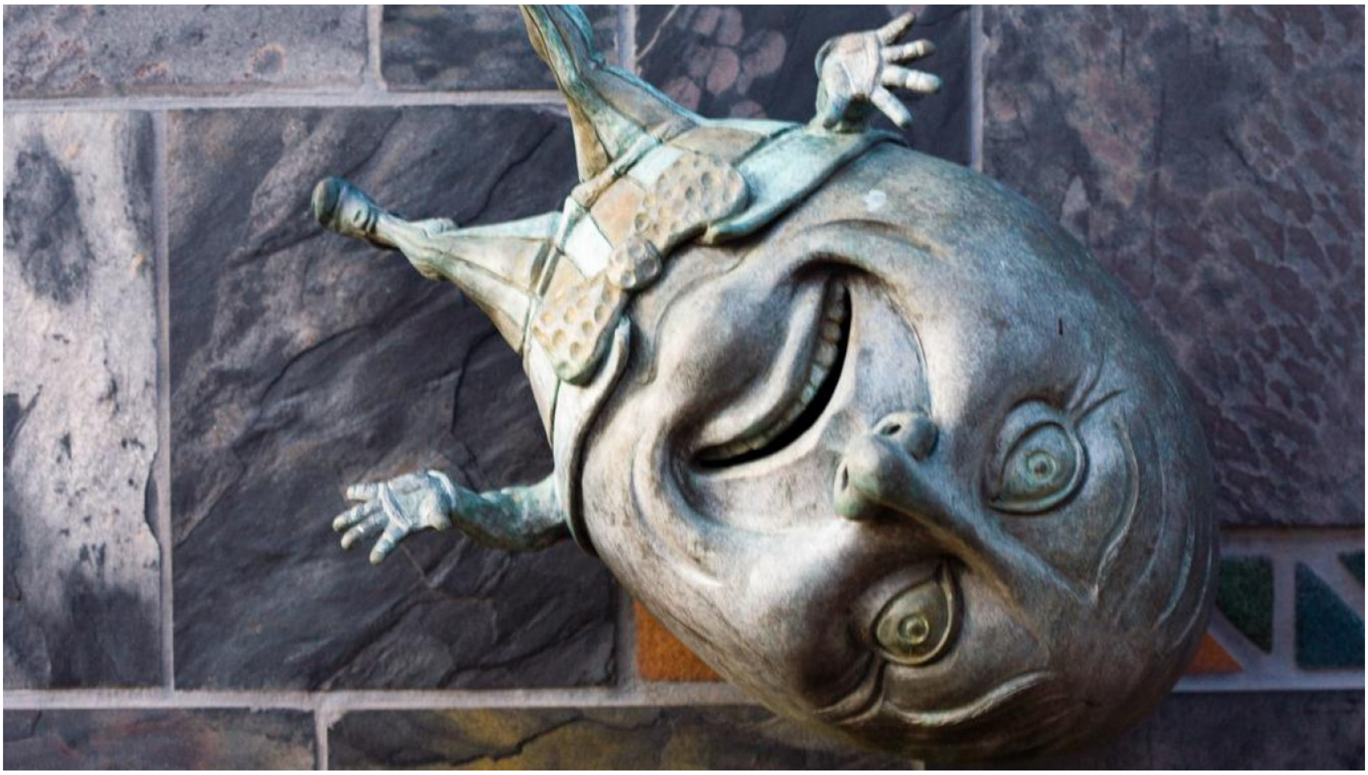
The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

# Treason Through the FSB Looking Glass

## Why 'espionage' arrests at the heart of Russia’s security services are not all that they seem

By Mark Galeotti

January 30, 2017



**Aturkus / Flickr**

Is espionage or bureaucratic politics behind the leak of news about the arrests of a number of Russian computer security specialists? As often the case in Russia, the story is murky; it is probably a bit of both.

Last week it emerged that back in early December, the FSB had arrested two of its own, Colonel Sergei Mikhailov, head of the Second Operational Directorate of its Information Security Center (TsIB), and one of his subordinates, Major Dmitry Dokuchaev. They also detained Ruslan Stoyanov, head of investigations at Russia’s Kaspersky Lab cybersecurity company. It later emerged that this followed the arrest in October of Vladimir Anikeev, founder of the Shaltai-Boltai group, which hacked and released emails from and to several senior Russian officials, including Prime Minister Dmitry Medvedev.

All but Anikeev are reportedly being charged with treason, but for what? The leaks and rumors have presented an engagingly eclectic range of options. That Dokuchaev, reportedly a hacker named Forb, offered the choice between prison and the FSB, was part of Shaltai-Boltai (Russian for Humpty Dumpty: members of the group adopted monikers inspired by Lewis Carroll). That Mikhailov was in effect its “curator,” or else a spy, or at least received money from a foreigner, or wanted to undermine the Kremlin.

In the absence of any hard information, two broad narratives have emerged to explain the arrests. The first is that this is essentially a case of espionage, that they knowingly or unwittingly divulged state secrets to the Americans. The second is that this is instead one of the regular ‘*silovik* struggles’ take place within and around the security agencies, over resources, seniority or personality. The two need not, however, be mutually exclusive.

There is much to support the espionage angle. Although there is no evidence yet of any direct connection with the infamous leak of emails from Democratic National Committee servers, instead there is a potential link to an earlier intrusion into Arizona and Illinois voter registration databases. Mikhailov may have alerted US officials to FSB links with Russian server rental company King Servers, an alleged ‘nexus’ for these attacks.

"*It is difficult to track hacking through computer forensics alone. A human source ... could have helped the Americans confirm their judgments*"

This helps explain the affirmation in the unclassified US intelligence report on the DNC hacks that they had “high confidence” in their judgment about Russian interference. It is notoriously difficult to track the ultimate source of hacking through computer forensics alone. A human source or evidence through compromised communications — which the Americans could not even have hinted at in their report — could have helped confirm their judgments.

The arrests came just before the public release of the US report. With coordinated accounts appearing in four news outlets, including firsthand accounts of Mikhailov’s dramatic arrest during a meeting, it is clear that the Kremlin is behind last week’s accounts. But having kept the story under wraps for almost two months, why break it now?

It could be to suggest that any hacking was not done on the Kremlin’s orders although Donald Trump is unlikely to need any such assurances, and the US intelligence community is unlikely to believe them.

**Related article**: Second FSB Agent Arrested for Treason Revealed as Notorious Hacker

Instead, though, the timing may be a result of the perennial hidden politics of this deeply opaque regime.

As often is the case, frivolous conspiracy theory served as an indicator of serious politics. In a classic exercise in mirror-imaging following the way WikiLeaks has been used by Russian intelligence, the nationalist Tsargrad TV outlet claimed that the CIA was behind Shaltai-Boltai, and used it to leak potentially embarrassing emails from Russian politicians. Indeed, it claimed Mikhailov and his boss Andrei Gerasimov wanted to work with Sberbank, and its CEO, German Gref — something of a hate figure to the ultranationalists — to capture enough 'big data' on Russians to be able to manipulate public opinion and thus elections, and not in the Kremlin's interests.

So far, so paranoid. Gerasimov, TsIB's long-serving head, was under a cloud, and has reportedly already been pushed into early retirement. But this likely owes more to increasing conflict over control of the state's cyberintelligence capacities.

TsIB has quietly emerged as a pivotal agency, overseeing in the name of fighting cybercrime almost every aspect of domestic operations and, given that hacking knows no geography, implicitly also foreign activities. This is a massive economic opportunity, for payoffs but also exerting pressure on the country's financial and telecoms sectors.

It is also a source of power. TsIB already dominates the analogous Directorate K of the Ministry of Internal Affairs (and until 2006, Stoyanov worked in the USTM, Moscow police's Special Technical Activities Directorate, the local branch of Directorate K). It also has close links with Russia's two main cybersecurity companies, Kaspersky and Group-IB.

In the circumstances, let's see if TsIB retains its pivotal role and if so, whose ally or client replaces Mikhailov. This could be a slap down for an overreaching FSB, but is more likely a sign that, in a recognition of the growing importance of hacking and data access as a political tool and economic honey pot, the Kremlin wants to make sure TsIB is in the 'right' hands.

*Mark Galeotti is a senior researcher at the Institute of International Relations Prague.*

*The views expressed in opinion pieces do not necessarily reflect the position of The Moscow Times.*

Original url: https://www.themoscowtimes.com/2017/01/30/treason-through-the-looking-glass-a56975