The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Hacking Controversy Highlights Kremlin's Self-Destructive Approach

The cybersecurity debate is a metaphor for a wider problem for Moscow and the West, undermining last efforts to find grounds for cooperation.

By Mark Galeotti

May 19, 2021

Alexander Avilov / Moskva News Agency

It's getting hard enough to distinguish between the purely criminal and the state-inspired or -initiated in the physical world. It's even harder in cyberspace, and yet this is also one of the key territories for future conflict and potential collaboration between Russia and the West. More broadly, though, this is also a metaphor for the self-destructive ways that the Kremlin's attempts both to enjoy the fruits of cooperation and also use it for its own zero-sum purposes — and as a result, gain neither.

Bad reputation…

In early 2020, hackers from, it is believed, Russia's Foreign Intelligence Service (SVR), got into the systems of SolarWinds, an important US information technology firm with clients including many government agencies. They used their access to add 'back doors' into the systems of its clients, used to spy on their communications. For months, they had unfettered access to unclassified but nonetheless useful data from up to 18,000 of SolarWinds's customers, not least Treasury and the Department of Homeland Security.

It was a massive operation, a real cyberespionage coup, whose full implications are not yet clear. Nonetheless, it was espionage, not sabotage: no systems were damaged, no files corrupted, no subsequent leaks made with political intent. It was, to be blunt, the kind of operation one presumes America's NSA or Britain's GCHQ is every day trying to carry out in Russia.

Nonetheless, the U.S. political class responded with a barrage of escalatory rhetoric. It was described as 'destructive' in its impact on the US military (it wasn't), as 'virtually a declaration of war' (it wasn't) and the 'cyber equivalent of Pearl Harbor' (still wasn't). Whether or not the new administration accepted these overheated claims, or whether it was simply making sure it could not be accused of being 'soft on Russia,' it used the opportunity of a package of sanctions connected to meddling in the 2020 elections and the imprisonment of Alexei Navalny also to institute measures linked to the SolarWinds case, even if pretty token ones.

It reflects the way that every Russian-related cybercrime is all too easily seen as a Kremlin operation, though. Russian-based hackers appear to have been behind a later attack on Colonial Pipelines, leading to fuel shortages and hoarding up the eastern seaboard, and the alleged payment of a $5 million ransom.

Again, the first claims were that this was nothing short of state-sponsored sabotage, that 'nothing happens in Russia from a cybercrime perspective without it going through the Kremlin.' Fortunately, this time the Biden administration moved quickly to push back against suggestions of a Kremlin link, but for some politicians and commentators, this was simply to prevent it derailing the forthcoming Biden-Putin summit.

Related article: Can the U.S. Still Cooperate With Russia's Security Agencies?

Assumptions that Russia is a 'mafia state' where the Kremlin runs the underworld, online or on the streets, reflect serious misunderstandings of the complexities of the situation. Nonetheless, it is easy enough to see how they emerge, when the security agencies use gangsters as proxy assassins, and when certain major hacking groups do indeed seem to have a degree of impunity, whether because of corruption or collaboration.

As a result, when Russia does seek to present itself as a partner or seek to advance what may appear to be positive measures — and it is encouraging the notion of a global cybersecurity treaty through the United Nations, that is self-interested but not wholly without merit — it inevitably is treated with suspicion and disdain. And, of course, this only fosters a paranoid and embittered sense amongst the Russian security elites in particular, who interpret this not

as a response to their own past adventures, but as 'proof' of some Russophobic plot to demean and marginalise their country.

In other words, the cybersecurity debate is a metaphor for a much wider problem for both Moscow and the West, one that undermines any last positive efforts to find grounds for cooperation, and exacerbates an already-tense relationship.

Bad decisions

The irony is that the Kremlin itself is increasingly worried about hacking. Back in the 1990s, even the earlier 2000s, Russian cybercriminals would largely focus on the West. In part, this was patriotism, in part, devilry, but above all it was simply that this was where the targets were and this was where the money was.

Related article: U.S. Government Confirms Cyberattack After Reports of Russia-Linked Hacking

This has been changing, though. Last year, General Prosecutor Igor Krasnov reported that in the period 2016-20, attacks in Russia had risen twenty-five-fold. More than anything else, this can be attributed to the way that the rapid expansion in online banking, trading and services in Russia means it now offers much more tempting opportunities. Indeed, Russia is now also being targeted by foreign cybercriminals, including well-organized groups from China and possibly also North Korea.

Of course, the security apparatus tends to view such cases purely through its own interests and assumptions. Figures such as Sergei Naryshkin, director of the SVR, and Nikolai Patrushev, secretary of the Security Council, have asserted that the USA is the main source of attacks, especially on Russia's critical information infrastructure. While there are intrusions into Russian systems, both from criminal hackers and the NSA, the suggestion that this is primarily driven by geopolitics is very questionable. Every government and state faces similar challenges in the modern, networked era.

This is something well understood by many professionals in Russia, especially within the corporate cybersecurity field and the Directorate K of the Ministry of Internal Affairs (MVD), responsible for computer crimes. Their activities would genuinely benefit from closer cooperation with the West. But here's the problem: the Russian state also has a track record of using, even recruiting hackers to conduct hostile operations against the West.

Originally, this was essentially by the FSB encouraging 'patriotic hackers' or by offering a degree of indulgence to those criminals who chose the 'right' targets, such as Estonia in 2007, Georgia in 2008 and Ukraine since 2014. Over time, though, this moved to the direct commissioning of specific operations and even recruiting hackers into the ranks of the FSB's Information Security Centre, with at best mixed success.

Yet it is also the FSB that the Kremlin has made the sole gatekeeper to cybercrime cooperation — according to Western police liaisons in Moscow, the MVD cannot or will not take the lead. As Andrei Soldatov has noted, what can be done, "if all the doors to cooperation, both government and private, remain shut and sealed, except the door of the FSB — the very

agency which is accused of carrying out repressions, poisonings, and cyber-attacks?"

The answer is, not a lot. Even in the post-Navalny (poisoning and imprisonment) era, there is a case to be made for better law-enforcement cooperation between Russia and the West as offering pragmatic benefits on both sides. However, this depends on Moscow having a willingness to treat it as separate from the covert subversion, intelligence operations and rhetorical theatricalities of the day-to-day political war — and the West being willing to trust this.

Related article: EU, UK Slap Sanctions on Russian Spies for Hacking German Parliament

Bad outcomes

After all, up to now cooperation in law enforcement has been used by the Kremlin more than anything else as a gambit. Intelligence sharing on terrorist threats was often hijacked by a desire to demonize Chechens and others opposed to Moscow and get the West to do Russia's dirty work. Just as with Interpol, bilateral cooperation was frequently used to try and pressurize emigres who had turned against Putin. More broadly, attempts were made to try and make cooperation a transactional process, a prize for acceding to Russian interests in some other situation.

There are still some areas where it works, from dealing with especially heinous crimes such as child abuse, or where it builds on long-term relationships, such as Finland's in north-western Russia. There is also scope for low-level, technical cooperation, especially in response to requests from courts and magistrates. More generally, though, while many professionals on both sides would want to cooperate, the process has been poisoned by mutual mistrust and by Moscow's efforts to manipulate the process.

This is a depressingly common pattern. The Kremlin's attempts to have its cake and eat it — to benefit from the fruits of cooperation and also to abuse its terms and etiquette for immediate political advantage — means no cake for anybody.

This stretches across the board. Moscow's geopolitical adventurism has led to sanctions affecting Russian business and educational links, however much participants on both sides would like to collaborate. Russian journalists, most of whom are still serious professionals, face the assumption that they are all toxic propagandists.

Most of all, those Russian diplomats keen to preserve vital international connections find their ministry side-lined by the security interests, and their work undermined by those seeking a momentary hit of patriotic defiance (such as the infamous #smalldickenergy tweet directed at Lithuania) or more eager to engage in self-destructive squabbles (such as recent disputes over U.S. and Czech diplomatic representation).

So this is the outcome: the Kremlin's eagerness to score short-term victories and its determination to frame its relationship with the West as competitive not only helps empower hawks in the West who say no meaningful cooperation with Moscow is possible or desirable, but rebound to hurt Russia's own interests.

This article was first published by Raam op Rusland.

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

Original url:
https://www.themoscowtimes.com/2021/05/19/hacking-controversy-highlights-kremlins-self-destructive-approach-a73943