



RUSSIA REFORM MONITOR

The American Foreign Policy Council's Review of
Russian Government Actions and U.S. Policy

Russia Reform Monitor No. 2422

October 27, 2020 **Matt Maldonado, Ilan I. Berman, Amanda Hardy**

Related Categories: Cybersecurity and Cyberwarfare; Democracy and Governance; Economic Sanctions; Human Rights and Humanitarian Issues; Global Health; Europe; Middle East; Russia

ERASING THE HISTORY OF SOVIET REPRESSION

According to Russian language outlet *Fontanka*, a famous monument to Soviet-era dissidents has been removed in Saint Petersburg. Since 2015, 23 Rubinstein Street had been home to sixteen memorial plaques, each dedicated to a Soviet dissident who had previously resided at the site. They were erected as part of the Last Address Project, an initiative designed to commemorate victims of Communism all over Russia. The building itself is known as Dovlatov's House, for the "samizdat" (self-publishing) writer who lived in it for over thirty years. Building administrators took the plaques down after residents complained they were not consulted about their display and that they caused "the house to look like a cemetery." Sources told *Fontanka* the residents will decide the ultimate fate of the plaques at a later date. (*Meduza*, October 19, 2020)

PANDEMIC FATIGUE SETS IN AMONG RUSSIA'S LEADERS

As a COVID-19 resurgence takes place in the United States and Europe, policymakers in Russia's largest city are balking at the idea of reimposing strict preventative measures to protect against the virus. While the country recently smashed its single-day infection record of 16,000 confirmed cases, the Mayor of Moscow has already come out and asserted that no harsh economic restrictions are planned.

The decision to keep life normal is a political one. During the height of lockdowns in May, President Vladimir Putin registered his worst approval rating in twenty years, prompting leaders to reverse course before a referendum vote scheduled for the end of June. With parliamentary elections on the horizon next year, politicians seeking reelection cannot afford the economic consequences associated with a strict shutdown similar to what was implemented earlier this year. (*Radio Free Europe/Radio Liberty*, October 21, 2020)

EU SANCTIONS GRU CHIEF OVER 2015 GERMAN HACK

In response to the German claim that Russian military intelligence hacked the emails of Chancellor Angela Merkel, the EU has levied sanctions on GRU Chief Igor Kostyukov. The bloc also sanctioned members of the GRU Special Operations Division, believed to have been the unit that actually carried out the hack. According to German authorities, Merkel and other political leaders had information and other data stolen when the GRU targeted the country's parliament in 2015. One of the accused hackers, Dmitri Badin, is believed to also be a member of Fancy Bear, the group that allegedly hacked email servers of the Democratic Party during the 2016 U.S. elections. (Reuters, October 22, 2020)

GRU HID NOVICHOK PRODUCTION: BELLINGCAT

According to a year-long investigation by Bellingcat, Russian production of the Novichok nerve agent did not cease after the country claimed to have destroyed its stockpiles in 2017. Novichok is the nerve agent believed to have been used to poison ex-spy Sergei Skripal in 2018 and opposition activist Alexei Navalny earlier this year - incidents in which the Kremlin denies involvement. Bellingcat claims production of the nerve agent was able to continue under the cover of civilian research. Phone records point to an open channel between Russian military intelligence (GRU) and civilian labs working clandestinely to manufacture the chemical weapon. One scientist in particular, Sergei Chepur, exchanged over 60 calls and texts with members of the GRU's infamous Unit 29155, believed to be behind the recent string of Novichok attacks. (*The Moscow Times*, October 23, 2020)

AEROFLOT VISAS CANCELLED AFTER IPHONE SCHEME REVELATIONS

The Department of Justice has charged ten Russian nationals with organizing a scheme to smuggle \$50 million worth of stolen Apple products into Russia. Between August and December of last year, the thieves reportedly smuggled over 1,235 pieces of consumer electronics, including stolen iPhones, iPads, and Apple Watches. Eight of the ten individuals charged are now in custody, while two are currently on the run from authorities. Investigators believe all ten smugglers were crewmembers for Aeroflot, Russia's national airline. As retaliation, the State Department has revoked the U.S. visas of 113 current and former Aeroflot employees. In an official statement, the Russian airline denied having ever employed any of the accused smugglers, but said it is working with the Russian Embassy in Washington, DC to clarify the matter. (*The Moscow Times*, October 20, 2020)

TREASURY SANCTIONS RUSSIA OVER 2017 SAUDI OIL HACK

The U.S. Office of Assets Control sanctioned a Russian-controlled state research center last week for supporting cyber attacks involving the Triton malware, which was used to remotely cripple infrastructure systems. In 2017, Triton was deployed to target Saudi oil refineries along the Red Sea. The malware was blocked from causing significant damage by an automatic shut-off, but the attempt put Western cybersecurity experts on alert. In 2019, the same malware was used to probe electrical utilities in the United States in search for vulnerabilities. The cybersecurity industry considers the use of Triton to be "the most dangerous threat activity publicly known." (U.S. Department of Treasury, October 23, 2020)