



RUSSIA REFORM MONITOR

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

Russia Reform Monitor 2281

December 26, 2018 **Ilan I. Berman, Margot van Loon**

Related Categories: Cybersecurity and Cyberwarfare; Democracy and Governance; Science and Technology; Terrorism; NATO; Caucasus; China; Iran ; Russia; Ukraine

HOW MOSCOW PREGAMED THE KERCH STRAIT CRISIS

A private intelligence firm has uncovered evidence that Russia orchestrated last month's Kerch Strait crisis well in advance, laying the groundwork for the attack on Ukrainian naval vessels with an offensive cyber operation. Analysts from Stealthcare report that Carbanak, a state-backed group of Russian hackers, launched an aggressive phishing campaign two months ago on Ukrainian government agencies possessing information about the country's foreign affairs and naval activity. While Stealthcare refrained from sharing details due to the investigation's sensitivity, they observed that another hacker cell, the Gamaredon Group, organized a separate attack known as "Pterodo" on November 20th that enabled covert backdoor access to Ukrainian government and military computers. A second wave of the Pterodo attack hit Kyiv's systems on November 26th – the same day that the Russian navy attacked the Ukrainian ships. (*Defense One*, December 7, 2018)

AN OLIVE BRANCH ON THE INF

The Russian Ministry of Foreign Affairs has confirmed its willingness to engage in negotiations to halt U.S. withdrawal from the Intermediate-Range Nuclear Forces (INF) Treaty. While Russia has not formally responded to U.S. demands that it scrap its non-INF compliant 9M729 missiles and launchers, Foreign Ministry official Vladimir Yermakov has announced that the Kremlin is interested in meeting with American officials in an interagency format to map out a way forward.

Russian officials, however, have been quick to outline the limits of their willingness to cooperate. In his comments, Yermakov emphasized that unilateral American inspections of Russian sites are categorically off the table. He did intimate, though, that Moscow may be amenable to a mutual inspection regime as a way of assuaging U.S. concerns. (Reuters, December 14, 2018)

IRAN SANCTIONS DETER RUSSIAN INVESTMENT

Moscow and Tehran may still be steadfast strategic partners, but the Trump administration's re-imposition of sanctions on Iran is nonetheless beginning to impact the scope of ties between the two countries. Russia's state-owned oil giant, Rosneft, is now reportedly pulling out of a \$30 billion joint investment with the National Iranian Oil Company due to the elevated business risk posed by the reinvigorated sanctions. Nor is Rosneft the first Russian energy company to retreat from Iran; Zarubezhneft, another significant oil conglomerate, has also pulled out of Iranian projects since the sanctions hit on November 5th, while LUKoil has announced it will not sign further contracts with Tehran until the sanctions are lifted. (*The Moscow Times*, December 13, 2018)

A TERROR STING IN THE CAUCASUS

Russian authorities have apprehended a group of suspects accused of financially supporting terrorist organizations. The suspects were detained in the republics of Chechnya, Dagestan, and Ingushetia, as well as in the Moscow region, during a joint operation carried out by the Federal Security Service, the Russian Investigative Committee, and the National Guard. Collectively, the suspects are accused of having provided some 38 million rubles (approximately \$570,000) to the Islamic State and the Al-Nusra Front terrorist groups since 2010. (*Radio Free Europe/Radio Liberty*, December 13, 2018)

CHINA COVETS RUSSIAN WATER

China's northern regions are increasingly parched, and Beijing is looking to its northern neighbor for a solution. According to Russia expert Paul Goble, the Russian-Chinese Strategic Investment Foundation has sent a letter to Russian premier Dmitry Medvedev formally requesting that he "support a Chinese plan to construct a canal to divert water from the Altay region to China." The RCSIF's plan, which was first floated publicly this summer, envisions a 1,200-1,500 kilometer pipeline to be constructed between the countries. The first stage, completion of which would be envisioned by 2026, would have the capacity of carrying 600-700 million cubic meters of water from Russia to China yearly. The second stage, which would last until 2014, would see that volume rise to between 1.8 and 2.4 billion cubic meters annually.

Such a move, Chinese officials say, has "received political support" from Russian authorities - at least preliminarily. But, Goble notes, realization of the plan would carry real risks for the Kremlin, because "it seems certain to infuriate Russians and Siberians alike." For their part, Russian experts say that the plan is feasible so long as the scheme doesn't account for more than one percent of Altay's overall water. (*Window on Eurasia*, December 11, 2018) **HOW MOSCOW PREGAMED THE KERCH STRAIT CRISIS**

A private intelligence firm has uncovered evidence that Russia orchestrated last month's Kerch Strait crisis well in advance, laying the groundwork for the attack on Ukrainian naval vessels with an offensive cyber operation. Analysts from Stealthcare report that Carbanak, a state-backed group of Russian hackers, launched an aggressive phishing campaign two months ago on Ukrainian government agencies possessing information about the country's foreign affairs and naval activity. While Stealthcare refrained from sharing details due to the investigation's sensitivity, they observed that another hacker cell, the Gamaredon Group, organized a separate attack known as "Pterodo" on November 20th that enabled covert backdoor access to Ukrainian government and military computers. A second wave of the Pterodo attack hit Kyiv's systems on November 26th – the same day that the Russian navy attacked the Ukrainian ships. (*Defense One*, December 7, 2018)