



RUSSIA REFORM MONITOR

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

Russia Reform Monitor No. 2326

August 8, 2019 **Margot van Loon**

Related Categories: Cybersecurity and Cyberwarfare; Democracy and Governance; Human Rights and Humanitarian Issues; Iran; Russia

THE SUFFOCATION OF RUSSIA'S DEFENSE INDUSTRIAL BASE

Although the \$300 billion spent to date by the Russian government on weapons modernization may sound like a boon for the country's state-run defense industry, it has in fact created a massive debt burden and a crisis of confidence among domestic producers. Since the government only releases funds for the systems it buys after they are completed, producers are forced to borrow money from the biggest state-owned banks to cover costs until the payment comes through – often at high interest rates. This policy, combined with general inefficiencies and poor management, has created an unsustainable financial situation.

Speaking at a defense conference in July, Deputy Prime Minister Yuri Borisov warned that the entire industry is now carrying two trillion rubles (more than \$30 billion) worth of bad debt, a loan portfolio whose service payments exceed cumulative annual profits. Although analysts estimate that 600-700 billion rubles of debt forgiveness would be needed for the industry to return to normal, the government has only agreed to write off 200 billion (\$3 billion). And as the government winds down its modernization program after a decade of ambitious spending, it will soon become even harder for Russia's defense giants to pay back their loans. (*Bloomberg*, July 15, 2019)

RUSSIA TO BACK EU TRADE VEHICLE WITH IRAN

As the 2015 Iran nuclear deal lurches towards potential collapse, Moscow is considering a new gesture of support for the Iranian government in hopes of salvaging the agreement. Kremlin spokesman Dmitry Peskov has suggested that Russia may join INSTEX, a financial workaround designed by the European Union to facilitate trade with Iran without running afoul of the crushing sanctions regime reimposed by the Trump administration last year. Peskov also suggested that the channel expand to include oil transactions – a provision sought by Tehran and vigorously opposed by the White House. So far, the ten EU countries that have committed to INSTEX to date have been reluctant to consider adding oil to the vehicle's umbrella, which remains limited in theory to trade in humanitarian goods. However, EU officials expressed an openness to including Russia in the arrangement once it is fully operational. (*Financial Times*, July 29, 2019)

LUNAR CONSPIRACY GAINS GROUND

On July 20th, the United States commemorated the 50th anniversary of the Apollo 11 moon landing, but an increasing number of Russian citizens believe that this mission never took place. According to a poll by state-run VTSIOM, only 24 percent of adult respondents believe that the U.S. actually succeeded in sending astronauts to the moon, and 57 percent firmly deny that the landings took place – an increase of seventeen percentage points since the poll was first conducted seven years ago.

The appeal of the lunar conspiracy appears to have only taken root among Russians after the collapse of the Soviet Union, and Russian space enthusiast Vitaly Yegorov hypothesizes that the skepticism stems from wounded pride: "no one wants to feel themselves a loser nation. So this denialism is not so much revenge, but it brings some calm to people: they beat us in Hollywood, but not in space." Yegorov further asserts that government propaganda demonizing the U.S. and the West has reinforced the idea that the U.S. is a "lying nation." Even though Russian President Vladimir Putin has dismissed the conspiracy theory in public, other senior officials have made comments that fuel it; space agency ROSKOSMOS head Dmitry Rogozin famously joked that "we've given ourselves the task of going there to check whether [the Americans] have been there or not." (*Radio Free Europe/Radio Liberty*, July 19, 2019)

FSB CONTRACTOR HIT BY MASSIVE DATA BREACH

Not even the Russian security services are safe from cyber intrusions. On July 13th, a contractor working for the country's Federal Security Service (FSB) became the latest online victim when a hacking group known as 0v1ru\$ breached its servers and made off with 7.5 terabytes of data about various FSB projects dating back to 2009. Noteworthy schemes revealed by the subsequent leak of these documents include a plan to deanonymize TOR, likely as a way of targeting political dissidents who use the "deep web" browser to protect their identities. (*EnGadget*, July 21, 2019)