AMERICAN FOREIGN POLICY COUNCIL


# Russia Reform Monitor No. 2274

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

**REGAINING AMERICA'S EDGE AGAINST RUSSIA (AND CHINA)**
A new bipartisan report has concluded that the United States is not investing enough in defense, and that it "might struggle to win, or perhaps lose, a war against China or Russia." The study was released by the National Defense Strategy Commission, a panel appointed by Congress to evaluate President Trump's 2018 *National Defense Strategy* (NDS). The Commission determined that, despite the NDS's lofty modernization goals, the Pentagon's acquisition system remains too risk-averse and slow to innovate to actually achieve its objectives. The report highlights a series of next-generation capabilities that require significant investment in order to reliably counter other major-power adversaries in combat, and it recommends that Congress lift budget caps currently imposed on defense spending in order to do so. (*Washington Post*, November 14, 2018)

**A DIFFERENT KIND OF RUSSIA HACK**
An anonymous Russian cyber expert has come forward claiming that the Russian Security Service (FSB) attempted to target a major British government system not long ago. The expert, an IT specialist employed by the contractor that manages the United Kingdom's visa system, alleges that the FSB approached him because of his access privileges, asking for network maps and visas for "a couple of guys who need to visit the UK" – a mysterious request that investigative outlet Bellingcat speculates may be a reference to the two men accused of carrying out the Novichok nerve agent attack in Salisbury earlier this year. In exchange for his assistance, the FSB offered to expedite the man's own immigration application from Mongolia to Russia; he balked only when the handlers demanded that he create a cyber backdoor to allow them unauthorized access to the system. (*The Daily Beast*, November 16, 2018)

**THE FSB VERSUS INTERNET COOPERATION**
Russia's premier intelligence agency is reportedly blocking the country's space agency from participating in a sweeping global satellite communications system, citing national security concerns. The "OneWeb" project, founded by former Google official Greg Wyler, envisions the stationing in orbit of 900 miniature satellites to provide global coverage for high-speed Internet and communications. Russia's space agency, ROSKOSMOS, was originally a key partner in the multi-billion dollar project, having signed a participation agreement with OneWeb back in 2015. But now, the FSB is actively opposing the venture, declaring it a "threat to national security." It is now up to President Vladimir Putin to end the stalemate, and formally decide whether Russia will take part in the OneWeb venture. ( *Radio Svoboda*, November 13, 2018)

**NEW FACTORS IN THE RUSSIAN-IRANIAN ALLIANCE**
For years, U.S. policymakers have speculated about whether it might be possible to sever the long-standing strategic ties between Moscow and Tehran. However, repeated efforts spanning multiple administrations have failed to drive a meaningful wedge between the two countries. Yet today, Russia's expanding ties to the countries of the Middle East and North Africa are injecting new variables into the traditionally robust bilateral partnership.

According to Oxana Gaman-Golutvina of the prestigious Moscow State Institute for International Relations, the Kremlin is now seeking to balance its longstanding Shi'ite-centric policy in the Middle East with greater outreach toward the Sunni states of the Gulf and Levant. Russia's government, Gaman-Golutvina told the most recent Abu Dhabi Strategic Debate earlier this month, has become convinced that doing so is essential to becoming a key strategic player in one of the world's most important regions. (*Arab News*, November 12, 2018)

**RUSSIAN HACKERS TARGET FOGGY BOTTOM**
Hackers affiliated with the Russian government have engaged in a phishing scheme aimed at infiltrating the computer systems of U.S. government agencies, think tanks and private American businesses. According to two leading cybersecurity firms, CrowdStrike and FireEye, following a lull in activity surrounding the November midterm elections in the United States, a new Russian cyber offensive has attempted to infiltrate the computers of several public and private sector entities through emails purportedly originating from State Department spokesperson Heather Nauert. The messages contained attachments which, if opened, would install malicious software permitting the hackers to access the systems. The hackers, according to FireEye, are part of a group known as APT29, which foreign intelligence services have linked to Russia's main foreign intelligence service, the SVR. (Reuters, November 16, 2018)