AMERICAN FOREIGN POLICY COUNCIL

Russia Reform Monitor No. 2320

July 17, 2019 **Margot van Loon**

Related Categories: Cybersecurity and Cyberwarfare; Democracy and Governance; Energy Security; Europe Military; Human Rights and Humanitarian Issues; Intelligence and Counterintelligence; Public Diplomacy and Information Operations; Europe; Russia; Ukraine

RUSSIAN DISINFORMATION AND THE EU ELECTIONS
A report by the European Commission has confirmed that Russia conducted "continued and sustained" disinformation activities during the EU's Parliamentary elections this past May. Security Commissioner Julian King stated that, during the election, the number of Russian disinformation cases reached 1,000 (in comparison to 400 identified cases in May 2018, a non-election month), with themes including false narratives about the Notre Dame fire signifying the end of Christianity, the EU having Nazi roots, and the supposed negative economic effects of EU membership. King added that EU counter-disinformation measures implemented prior to the election likely had some positive deterrent effect, but that the EU needs to continue to adapt and improve its tactics as disinformation efforts evolve. (*Radio Free Europe/Radio Liberty*, June 14, 2019)

MOSCOW'S PASSPORT HANDOUT CONTINUES
Ukrainian citizens in separatist regions of the country have begun receiving Russian passports under a new Kremlin policy that critics say is designed to undermine the government in Kyiv. Russian Foreign Ministry official Oleg Agarkov confirmed that "several dozen" people picked up their passports in mid-June. He added that the first tranche of passport approvals numbered close to 1,200, and that his office is still processing more than 10,000 additional requests. The expedited passport program is an extension of the same policy implemented in May for residents of the Crimean Peninsula. The Ukrainian government has objected stridently to the handout, with Prime Minister Volodymyr Groysman calling them a "flagrant violation of all rights and morals" and saying that Ukraine "will never recognize the citizenship issued by an aggressor country." The EU has also condemned the policy, labeling it "another attack on Ukraine's sovereignty." (Berlin *Deutsche Welle*, June 14, 2019)

OUTRAGE AMONG RUSSIAN POLICE
The aftermath of the Ivan Golunov case, in which a botched sting operation against a journalist led to the ouster of two senior generals at the Ministry of Internal Affairs, has triggered an internal crisis within the Russian police force. Morale in the force is consistently reported to be low, with salaries and poor working conditions cited as common causes of dissatisfaction. However, some junior officers report a renewed desire to resign in the wake of the Golunov case, fearing that if even the most powerful members of the police force are vulnerable, then "simple mortals" on the force can no longer expect protection on the job. Others would prefer leaving for employment with the Russian National Guard, citing better working conditions and improved pay. When asked about the morale crisis, police union leader Mikhail Pashkin complained that "apparently our government no longer counts on the police and isn't investing in it." (*Window on Eurasia*, June 14, 2019)

THE ELECTRIC GRID AS BATTLEGROUND
A malicious group of hackers with likely ties to the Russian government has been discovered probing vulnerabilities in the U.S. electric grid. The group, known alternatively as Xenotime or Triton, established a reputation as one of the most dangerous cyber threat actors currently operating when it deployed malware at a Saudi oil refinery in 2017 designed to sabotage its safety and monitoring systems and trigger a deadly accident. Analysts at the Electric Information Sharing and Analysis Center (E-ISAC) and private security firm Dragos have been tracking Xenotime's activity within the U.S. grid, which so far includes scanning the networks of at least 20 separate systems since 2018. Although Dragos declined to attribute Xenotime's physical whereabouts, the group has been linked in the past to Moscow’s Central Scientific Research Institute of Chemistry and Mechanics.

The news of Xenotime's cyber lurking comes amid an escalating U.S.-Russian contest playing out in both countries' power grids. For years, the U.S. government has been aware of Russian incursions in U.S. critical infrastructure, including the implantation of malware that could sabotage key systems remotely. In a story published by the *New York Times*, several current and former government officials appeared to confirm that the U.S. is beginning to conduct similar clandestine offensive operations, planting malicious code in Russian infrastructure. This strategy is reportedly both a "shot across the bow" meant to deter Russia from further cyber aggression as well as to create tools for a meaningful U.S. response should Russia attack the U.S. grid as part of a greater actual conflict. "It has gotten far, far more aggressive over the past year... we are doing things at a scale that we never contemplated a few years ago," one official interviewed for the story confided.

President Trump authorized additional offensive authorities for U.S. Cyber Command last year, and multiple U.S. officials, including National Security Advisor John Bolton, have made public comments recently suggesting that the U.S. is adopting a more assertive approach in its cyber strategy. However, President Trump strongly denied the story's accuracy, taking to Twitter to call its publication a "virtual act of treason... ALSO, NOT TRUE." Moscow, for its part, did not directly confirm the reporting but did note that its critical infrastructure was being targeted from abroad. Kremlin spokesman Dmitry Peskov accused the United States of preparing "a cyber war" against Russia, and lamented that America had so far declined to join Vladimir Putin's multiple attempts to "lead the international community in preventing any and all forms of cyber crime." (*Wired*, June 14, 2019; *New York Times*, June 15, 2019; *The Daily Beast*, June 15, 2019; *Financial Times*, June 17, 2019)
