OFFICE *of* INTELLIGENCE *and* ANALYSIS

INTELLIGENCE IN BRIEF

23 JANUARY 2022 DHS-IA-IB-2022-00927

CYBERSECURITY

(U) Warning of Potential for Cyber Attacks Targeting the United States in the Event of a Russian Invasion of Ukraine

(U//FOUO) ***Scope Note:*** *This* Intelligence in Brief *provides strategic warning to federal, state, local, tribal, territorial, and critical infrastructure stakeholders of possible cyber implications related to current geopolitical events. The evolving nature of the current military escalation on Ukraine's border and ongoing dialogue between Moscow and Washington could influence Russia's actions, including options for targeting the United States. Given the nature of these events and the varied potential outcomes of ongoing security dialogues, this assessment could similarly evolve over the coming weeks and months.*

(U//FOUO) **We assess that Russia would consider initiating a cyber attack against the Homeland if it perceived a US or NATO response to a possible Russian invasion of Ukraine threatened its long-term national security.** Russia maintains a range of offensive cyber tools that it could employ against US networks—from low-level denials-of-service to destructive attacks targeting critical infrastructure. However, we assess that Russia's threshold for conducting disruptive or destructive cyber attacks in the Homeland probably remains very high and we have not observed Moscow directly employ these types of cyber attacks against US critical infrastructure—notwithstanding cyber espionage and potential prepositioning operations in the past.

- *(U)* Russia's cyber program is a key element of its broader view and military doctrine of "information confrontation"—a concept that values technical cyber operations and the psychological effects that can be achieved in an information environment, according to a 2021 NATO report. Moscow's cyber operations are designed to provide flexible options that can be used in both peacetime and wartime to achieve desired end states. Russia almost certainly considers cyber attacks an acceptable option to respond to adversaries because it lacks symmetrical economic and diplomatic responses, according to the Intelligence Community's 2021 Annual Threat Assessment.

(U) Prepared by the Cyber Mission Center. Coordinated with CISA, CYBERCOM, DIA, NGA, and ODNI.
For questions, contact DHS-SPS-RFI@hq.dhs.gov

- *(U)* Russia continues to target and gain access to critical infrastructure in the United States. During a campaign that started in March 2016, Russian Government cyber actors compromised US energy networks, conducting network reconnaissance and lateral movement, and collected information pertaining to industrial control systems, according to a Cybersecurity and Infrastructure Security Agency (CISA) alert. Separately, Russian state-sponsored cyber actors have successfully compromised routers, globally, and US state and local government networks, according to a CISA alert and a joint US-UK report.

- *(U//FOUO)* Russia has demonstrated the ability to conduct disruptive and destructive cyber attacks in other countries, using techniques that could be leveraged against US critical infrastructure networks. In both 2015 and 2016—progressively more capable year-over-year—Russian military intelligence (GRU) actors successfully launched cyber attacks against the Ukrainian power grid, temporarily interrupting the supply of power to hundreds of thousands of Ukrainians, according to a US indictment of GRU officers. In 2017, Russian actors used malware to target a Saudi Arabian refinery, infecting the safety systems and leading to the temporary shutdown of the plant, according to a Department of Treasury sanctions announcement.

(U) **Recent Relevant US Government Cyber Security Alerts**

- *(U//FOUO)* 18 January 2022: CISA Insights, *Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats*

- *(U//FOUO)* 11 January 2022: Joint CISA-FBI-NSA Cybersecurity Advisory, AA22-011A, *Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure*

- *(U)* 15 December 2021: CISA Insights, *Preparing for and Mitigating Potential Cyber Threats*

- *(U//FOUO)* 1 July 2021: Joint CISA-FBI-NSA-NCSC Cybersecurity Advisory, U/OO/158036-21, *Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments*

- *(U)* 22 October 2020: Joint CISA-FBI Cybersecurity Alert, AA20-296A, *Russian State-Sponsored Advanced Persistent Threat Actor Compromises US Government Targets*

- *(U)* 16 April 2018: CISA Technical Alert, TA18-106A, *Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices*
- (U) 16 March 2018: Joint DHS-FBI Technical Alert, TA18-074A, *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors*

Source, Reference, and Dissemination Information

Source Summary Statement	*(U//FOUO)* We assess that Russia would consider initiating a cyber attack against the Homeland if it perceived a US or NATO response to a possible Russian invasion of Ukraine threatened its national security. This assessment is made with **medium confidence** based on a media article about President Vladimir Putin claiming that the United States was not respecting Russian "redlines." We also base this assessment on CISA and media reporting on Russian compromises of US critical infrastructure networks; a US indictment of GRU officers; A Department of Treasury announcement of sanctions against a private sector Russian research institute; and media reporting of Russian destructive cyber attacks conducted against other countries' critical infrastructure. We further base this assessment on a NATO report on Russia's cyber program. *(U//FOUO)* We assess that Russia's threshold for conducting disruptive or destructive cyber attacks in the Homeland probably remains very high. This assessment is made with **medium confidence** based on a lack of observed cyber attack activity against the Homeland despite prior tensions, including public reports on US assistance to Ukraine; enhanced Forward Presence in the Baltic nations and Poland; US military aid to Ukraine; and Department of Treasury sanctions levied against Russian entities related to the Ukraine crisis.
Reporting Suspicious Activity	*(U)* **To report a computer security incident, either contact US-CERT at 888-282-0870, or go to https://forms.us-cert.gov/report/ and complete the US-CERT Incident Reporting System form.** The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.
Dissemination	*(U)* Federal, state, local, tribal, and territorial authorities and private sector security partners.
Warning Notices & Handling Caveats	*(U)* **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS. *(U)* All US person information has been minimized. Should you require US person information on weekends or after normal weekday hours during exigent and time sensitive circumstances, contact the Current and Emerging Threat Watch Office at 202-447-3688, CETC.OSCO@HQ.DHS.GOV. For all other inquiries, please contact the Homeland Security Single Point of Service, Request for Information Office at DHS-SPS-RFI@hq.dhs.gov, DHS-SPS-RFI@dhs.sgov.gov, DHS-SPS-RFI@dhs.ic.gov.