

# Treasury Sanctions Leader and Primary Member of the Cyber Army of Russia Reborn

 [home.treasury.gov/news/press-releases/jy2473](https://home.treasury.gov/news/press-releases/jy2473)



July 19, 2024

*The United States exposes the identity of and imposes sanctions on two members of the Russian government-aligned hacktivist group.*

WASHINGTON — Today, the United States designated **Yuliya Vladimirovna Pankratova (Pankratova)** and **Denis Olegovich Degtyarenko (Degtyarenko)**, two members of the Russian hacktivist group Cyber Army of Russia Reborn (CARR) for their roles in cyber operations against U.S. critical infrastructure. These two individuals are the group's leader and a primary hacker, respectively.

“CARR and its members’ efforts to target our critical infrastructure represent an unacceptable threat to our citizens and our communities, with potentially dangerous consequences,” said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. “The United States has and will continue to take action, using our full range of tools, to hold accountable these and other individuals for their malicious cyber activities.”

This designation follows several other recent U.S. Treasury actions to combat Russia-based cyber criminals. These include the May 7, 2024 designation of Dmitry Khoroshev, also known as LockBitSupp, who is a leader of the LockBit ransomware group, and the February 20, 2024 designation of LockBit affiliates Ivan Kondratiev and Artur Sungatov. According to

the Department of Justice, LockBit has targeted over 2,500 victims worldwide and is alleged to have received more than \$500 million in ransom payments. Furthermore, on January 23, 2024, the U.S. Treasury, in coordination with Australia and the United Kingdom, designated Alexander Ermakov, who was responsible for the October 2022 infiltration of one of Australia's largest private health insurers, Medibank.

## A focus on Critical infrastructure

---

Since 2022, CARR, which also uses the name Cyber Army of Russia, has conducted low-impact, unsophisticated DDoS attacks in Ukraine and against governments and companies located in countries that have supported Ukraine. In late 2023, CARR started to claim attacks on the industrial control systems of multiple U.S. and European critical infrastructure targets. Using various unsophisticated techniques, CARR has been responsible for manipulating industrial control system equipment at water supply, hydroelectric, wastewater, and energy facilities in the U.S. and Europe.

In January 2024, CARR claimed responsibility for the overflow of water storage tanks in Abernathy and Muleshoe, Texas, posting video of the manipulation of human-machine interfaces at each facility on a public forum. The compromise of the industrial control systems resulted in the loss of tens of thousands of gallons of water. Additionally, CARR compromised the supervisory control and data acquisition (SCADA) system of a U.S. energy company, giving them control over the alarms and pumps for tanks in that system. Despite CARR briefly gaining control of these industrial control systems, instances of major damage to victims have thus far been avoided due to CARR's lack of technical sophistication.



**Pankratova**, also known as YULiYA online, is a Russian cybercriminal and the leader of CARR. **Pankratova** commands and controls CARR's operations. **Pankratova** has acted as a spokesperson for CARR.



**Degtyarenko**, also known as Dena online, is a Russian cybercriminal and a primary hacker for CARR. **Degtyarenko** was behind the compromise of the SCADA system of a U.S. energy company. In early May 2024, **Degtyarenko** developed training materials on how to compromise SCADA systems and was possibly looking to distribute the materials to external groups.

OFAC is designating **Pankratova** and **Degtyarenko** pursuant to E.O. 13694, as amended, for being responsible for or complicit in, or having engaged in, directly or indirectly, cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that have the purpose or effect of harming, or otherwise significantly compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector.

## SANCTIONS IMPLICATIONS

---

As a result of today's action, all property and interests in property of the designated persons described above that are in the United States or in the possession or control of U.S. persons are blocked and must be reported to OFAC. In addition, any entities that are owned, directly or indirectly, individually or in the aggregate, 50 percent or more by one or more blocked persons are also blocked. Unless authorized by a general or specific license issued by OFAC, or exempt, OFAC's regulations generally prohibit all transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of designated or otherwise blocked persons.

In addition, financial institutions and other persons that engage in certain transactions or activities with the sanctioned individuals may expose themselves to sanctions or be subject to an enforcement action. The prohibitions include the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any designated person, or the receipt of any contribution or provision of funds, goods, or services from any such person.

The power and integrity of OFAC sanctions derive not only from OFAC's ability to designate and add persons to the SDN List, but also from its willingness to remove persons from the SDN List consistent with the law. The ultimate goal of sanctions is not to punish, but to bring about a positive change in behavior. For information concerning the process for seeking removal from an OFAC list, including the SDN List, please refer to [OFAC's Frequently Asked Question 897 here](#). [For detailed information on the process to submit a request for removal from an OFAC sanctions list, please click here.](#)

[Click here for more information on the individuals designated today.](#)

Use featured image

Off