U.S. Support for Connectivity and Cybersecurity in Ukraine

FACT SHEET

OFFICE OF THE SPOKESPERSON

MAY 10, 2022

Share

Leading up to and during Russia's unprovoked and illegal further invasion of Ukraine, the United States is supporting Ukraine's continued access to the Internet and to enhance Ukraine's cyber defenses. These efforts, coordinated across the U.S. government, include:

- The Federal Bureau of Investigation (FBI) has provided direct support to its Ukrainian national security and law enforcement partners, including briefing Ukrainian partners on Russian intelligence services' cyber operations; sharing cyber threat information about potential or ongoing malicious cyber activity; helping to disrupt nation-state efforts to spread disinformation and target the Ukrainian government and military; and sharing investigative methods and cyber incident response best practices. The FBI also has received threat intelligence and leads from its Ukrainian partners for action using the FBI's unique investigative and intelligence capabilities. FBI, State, and other U.S. government agencies have also assisted Ukraine with identifying and procuring hardware and software to support network defense.
- Technical experts funded by the U.S. Agency for International Development (USAID) are providing hands-on support to essential service providers within the Ukrainian government including government ministries and critical infrastructure operators to identify malware and

restore systems after an incident has occurred. This support builds on long standing USAID support building cyber resilience among regional utilities, particularly in the energy sector. USAID and the Department of State are also exploring new mechanisms to leverage the services offered by U.S. and Ukrainian cybersecurity service providers to support and reinforce the Government of Ukraine's own cyber defense efforts.

- USAID has provided more than 6,750 emergency communications devices, including satellite phones and data terminals, to essential service providers, government officials, and critical infrastructure operators in key sectors such as energy and telecommunications.
- The Department of Energy (DOE) and other interagency partners are working with Ukraine on efforts related to further integrating Ukraine's electrical grid with the European Network of Transmission System Operators for Electricity (ENTSO-E), including meeting cybersecurity requirements and enhancing the resilience of its energy sector. Full ENTSO-E integration is key to protecting Ukraine's financial, energy, and national security.
- The Cybersecurity and Infrastructure Security Agency (CISA) has exchanged technical information on cybersecurity threats related to Russia's unprovoked further invasion of Ukraine with key partners, including Ukraine. On February 26, CISA issued **an alert** providing technical details and mitigation guidance on destructive malware targeting organizations in Ukraine.
- Prior to February 2022, the U.S. government worked closely with Ukrainian government ministries and critical infrastructure sectors to support Ukraine's cyber resilience, including by providing over $40 million in cyber capacity development assistance since 2017. Among these efforts:
  - Beginning in 2020, USAID launched an ambitious $38 million cybersecurity reform program that will work over the next several years to strengthen Ukraine's cybersecurity legal and regulatory environment, build Ukraine's cyber workforce and strengthen course offerings at leading Ukrainian universities, and develop connections between critical infrastructure operators and private sector solution providers. This program has embedded more than 20 technical experts within the Government of Ukraine to bolster Ukraine's cyber response and recovery capabilities, and deployed cybersecurity software and hardware tools to ensure the resilience of critical infrastructure to physical and cyber attacks.
  - DOE has a long-standing relationship with the energy sector in Ukraine, including work with Ukrainian utilities to help enhance their cybersecurity posture. In the leadup to

with Ukrainian utilities to help enhance their cybersecurity posture. In the leadup to Russia’s further invasion of Ukraine, DOE, leveraging the expertise of our National Labs, worked with utilities to focus on potential near-term cybersecurity enhancements, while also continuing our work on long-term resilience efforts.

- The Treasury Department has worked with the National Bank of Ukraine (NBU), via the Software Engineering Institute (SEI), to support NBU’s Computer Security Incident Response Team (CSIRT) to improve cybersecurity information sharing in Ukraine’s financial services sector. Leading up to Russia’s further invasion of Ukraine, Treasury offered NBU assistance on specific cybersecurity issues while continuing to work on longer-term cybersecurity projects to better ensure the cyber resilience of Ukraine’s financial sector.
- From December 2021 to February 2022, cyber experts from U.S. Cyber Command conducted defensive cyber operations alongside Ukrainian Cyber Command personnel, as part of a wider effort to increase cyber resilience in critical networks. Cyber professionals from both countries sat side by side, looking for adversary activity and identifying vulnerabilities. In addition to this effort, the team provided remote analytic and advisory support aligned to critical networks from outside Ukraine.

The U.S. government’s efforts, closely coordinated with private sector and international partners, support Ukraine’s network defenders and telecommunications professionals, who continue to defend Ukrainian networks and repair infrastructure, often at direct risk to their lives. The United States condemns actions that block or degrade access to the Internet in Ukraine, which sever critical channels for sharing and learning information, including about the war.

TAGS

Bureau of Cyberspace and Digital Policy

Bureau of European and Eurasian Affairs

Cyber Security

Office of the Spokesperson

Ukraine

Related Articles

MAY 10, 2022

Attribution of Russia's Malicious Cyber Activity Against Ukraine

READ MORE

APRIL 15, 2021

Holding Russia To Account

READ MORE

MARCH 23, 2021

Secretary Antony J. Blinken and NATO Secretary General Jens Stoltenberg Before Their Meeting

READ MORE