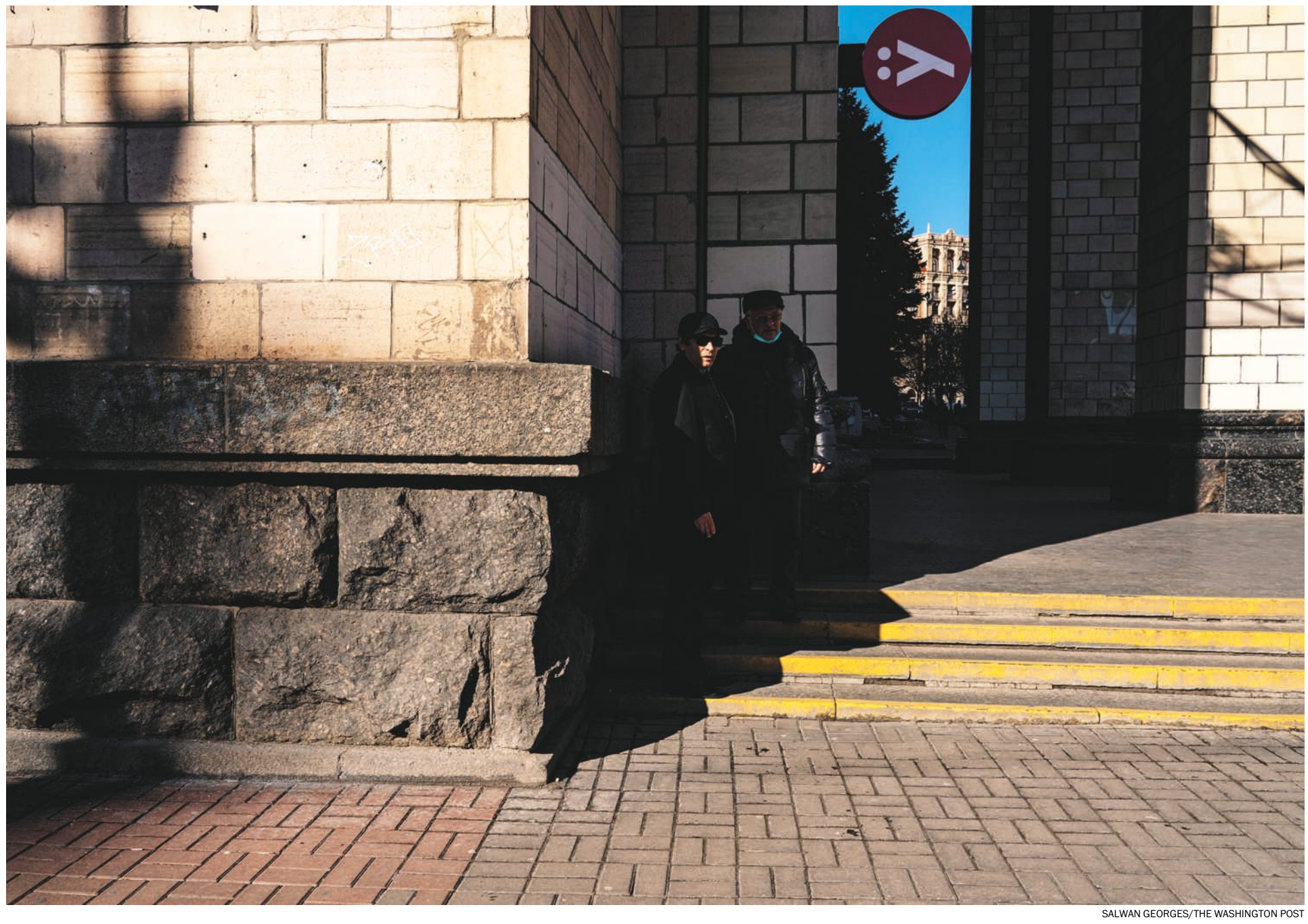
U.S.: Broad breach by Russian hackers likely in Ukraine

BY ELLEN NAKASHIMA AND ALEX HORTON



SALWAN GEORGES/THE WASHINGTON POST

Two men near the central square in Kyiv, Ukraine, on Tuesday. The Ukrainian government said that website of PrivatBank, the nation's largest commercial bank, was hit by a denial-of service attack Tuesday and that the websites of Ukraine's Defense Ministry and armed forces were also disrupted. U.S. officials say more cyberattacks could come.

Russian government hackers have likely broadly penetrated Ukrainian military, energy and other critical computer networks to collect intelligence and position themselves potentially to disrupt those systems should Russia launch a military assault on Ukraine, according to newly declassified U.S. intelligence.

Moscow could seek to disrupt Ukrainian entities that provide critical services such as electricity, transportation, finance and telecommunications — either to support military operations or to sow panic in an attempt to destabilize the country, according to a senior administration official who described the intelligence.

The U.S. government has determined only that Russia could undertake disruptive cyberactivity, not that it will, said the official, who like several others spoke on the condition of anonymity because of the matter's sensitivity. "We don't know that they have intention to do so," the official said. "But we have been working with Ukraine to strengthen their cyberdefenses."

A Kremlin spokesman did not respond to a request for comment.

On Tuesday, the Ukrainian government's Center for Strategic Communications and Information Security said that PrivatBank, the nation's largest commercial bank, was hit with a denial-of-service attack that temporarily interfered with customers' online banking transactions. Service was restored within hours, the government said.

The websites of Ukraine's Defense Ministry and armed forces were also disrupted, the agency said. It did not say who was behind the attacks.

Should the conflict with Ukraine escalate, officials fear there could be broader cyberattacks in retaliation to Western sanctions or other moves to support Ukraine.

The concern is so great that on Friday the White House's deputy national security adviser for cyber, Anne Neuberger, ran a tabletop exercise to ensure that federal agencies were prepared for Russian cyber-assaults that might take place in an escalating conflict with Moscow.

Such events could include a cyberattack against Ukraine, an attack against a NATO member or ransomware. "We wanted to prepare for every scenario," the official said.

President Biden on Tuesday said that "if Russia attacks the United States or our allies through . . . disruptive cyberattacks against our companies or critical infrastructure, we are prepared to respond."

Hackers working for Russia's Federal Security Service, or FSB, and its military spy agency, the GRU, have been spotted inside Ukraine's systems, according to a second U.S. official and another person familiar with the matter.

The U.S. government also has been warning critical industries in the United States to ensure their systems are as hardened as possible against cyberattacks as Russia could seek to disrupt electricity, gas and other systems. The Russians have in the past infiltrated the control systems of some American electric utilities, though no disruptions resulted.

Moscow has grown increasingly aggressive in cyberspace over the past decade, carrying out not only massive compromises of unclassified U.S. government email systems and interfering in the 2016 U.S. presidential election but also knocking out power temporarily in parts of Ukraine in December 2015 and then again in December 2016 in Kyiv, the Ukrainian capital.

Those attacks took place amid an escalating geopolitical confrontation between Ukraine — which was leaning toward the West — and Russia, which sought to pull the country back into its sphere of influence. In 2014, Russia invaded and annexed Crimea and then fueled a separatist conflict in eastern Ukraine, which continues.

Cyberattacks are a key weapon in Russia's larger effort to destabilize Ukrainian society, according to U.S. officials and analysts. Besides temporarily blacking out parts of Ukraine several years ago, Russian hackers also unleashed a computer virus in 2017 against Ukrainian government ministries, banks and energy companies. The malware, dubbed NotPetya, wiped data from computers and crippled services. It also spread beyond Ukraine, which officials say probably was not the Russians' intention, causing billions of dollars in damage globally.

"There's no doubt in my mind that Russia sees cyber as playing a significant role in its attempts to coerce and destabilize Ukraine," said a senior Western intelligence official. "Cyber has been a central part of Russia's military buildup. The challenge that the Ukrainians have is that the level of cyberactivity that's conducted against them day-to-day is already very high and the level of cyberactivity that's conducted against Ukraine is so much higher than any other nation would deal with and frankly would tolerate."

Russian hackers have designed malware expressly for use against Ukrainian computers. That has made it a challenge for the country's cyber defenders, and though they are more capable than they were eight years ago, they still struggle against Russian expertise, according to Western officials.

> *"If Russia attacks the United States or our allies through . . . disruptive cyberattacks against our companies or critical infrastructure, we are prepared to respond."*
>
> **President Biden**

"I think you would see cyberattacks as an enabler for whatever their operational plans are — as a way to isolate and paralyze the society by disrupting banks and other critical societal institutions," said Anthony Vassalo, a senior intelligence and defense researcher at Rand and a former senior U.S. intelligence officer.

Ukraine has improved its cyberdefense capabilities in critical infrastructure, said Tim Conway, an instructor at Sans, a private cyber training institute who was in Kyiv in December running an electric-sector cyberwar game to test the sector's preparedness. He said Ukraine, like other countries, needs to learn how to use manual operations at key locations to keep systems running in the event a cyberattack disrupts digitally controlled systems.

"This ability to operate through an attack is absolutely something that all countries should be looking at — not just Ukraine," he said.

Victor Zhora, deputy chairman of the State Service of Special Communications and Information Protection in Kyiv, acknowledged the challenge. Ukrainian cyberdefenses are "much better," he said. "But the attackers have developed their cyberweapons as well. That's why it's a constant game."

Ukrainian President Volodymyr Zelensky in December decreed the creation of a dedicated military cyber force, Zhora said. The Defense Ministry has cybersecurity specialists, he said, but "separate cyber forces never existed, and it's our task to create them this year."

Zhora said there has been "very fruitful cooperation with both U.S. and European institutions." The U.S. Agency for International Development has been running a long-term project in Ukraine to strengthen cybersecurity, train a cyber workforce and develop start-ups in cybersecurity to provide products and services.

Some U.S. agencies have been working with the Ukrainian government and critical sectors for years. Energy Department collaboration, for instance, stretches back to the attacks on the power grid in 2015. Several dozen U.S. Cyber Command personnel were in Ukraine, arriving in December to help shore up government and critical sector systems.

"The key piece is that we built some of the people-to-people connections to enable us to provide rapid incident support in the event of something significant," the senior administration official said. "The key is resilience."

If a crisis emerges, the U.S. government will try to provide support remotely, the official said. "You can do a lot without having people in a dangerous situation."

Last month, NATO and Ukraine signed an agreement to allow Ukraine to become a member of the alliance's malware information-sharing program. "What they need most at this moment is information," said a senior Western diplomat.

Ukraine is not a member of NATO, so it is not covered by the alliance's commitment to rise to the defense of a member in the event of an armed attack. But Neuberger said at a news conference in Brussels this month that at a minimum NATO would "call out any destructive or destabilizing cyberattacks," even against a nonmember such as Ukraine, to reinforce the U.N. norm against destructive attacks against critical services that civilians rely on.

Last month, hackers disrupted several Ukrainian government networks using malware that wiped data from the computers of several government agencies, rendering them inoperable until the systems could be rebuilt. Though no official attribution has been made, cyber analysts say the likeliest culprit is Russia. The FBI is helping with the investigation, Ukrainian officials said.

Microsoft, which operates cloud and software services, detected and helped mitigate the attack. Tom Burt, Microsoft's vice president for customer security and trust, said that after the wiper attack last month, the company set up a secure communications channel for the Ukrainian government to share information on a regular basis that could be useful to the government and critical infrastructure.

Mandiant is also investigating last month's wiper incident. The firm provides threat intelligence to a number of companies with operations in Ukraine and closely monitors the region for emerging threats. "We're taking all this information from places like Ukraine and filtering it and giving clients a comprehensive view of the threat picture," said John Hultquist, Mandiant's vice president of intelligence analysis.

Horton reported from Kyiv. Robyn Dixon in Moscow and David Stern in Kyiv contributed to this report.