The New York Times.- 20.12.2021

David E. Sanger and Julian E. Barnes

# U.S. and Britain Help Ukraine Prepare for Potential Russian Cyberassault

## *США та Великобританія допомагають Україні підготуватися до потенційній кібератаці з боку Росії*

*Сполучені Штати і Великобританія непомітно направили в Україну експертів з кібервійни, сподіваючись краще підготувати країну до того, що, на їхню думку, може стати наступним кроком президента Росії В. Путіна - кібератаки, що руйнують електромережі, банківську систему та інші важливі компоненти економіки та уряду України, які стримати особливо складно. На думку автора американського видання, у кіберсвіті немає ні широкого консенсусу щодо того, що є актом війни, ні згоди щодо того, наскільки глибоко В. Путін може завдати Україні шкоди, не викликавши реакції Заходу.*

*https://www.nytimes.com/2021/12/20/us/politics/russia-ukraine-cyberattacks.html?searchResultPosition=7*

Russia has attacked Ukraine's power grid in the past, and experts say Moscow might take similar steps as it masses troops along the border.

U.S. and Britain Help Ukraine Prepare for Potential Russian Cyberassault

Russia has attacked Ukraine's power grid in the past, and experts say Moscow might take similar steps as it masses troops along the border.

The Ukrainian power grid was built in the days of the Soviet Union and is connected to Russia's, making the software as familiar to the attackers as to its operators.

The Ukrainian power grid was built in the days of the Soviet Union and is connected to Russia's, making the software as familiar to the attackers as to its operators.Credit...Valentyn Ogirenko/Reuters

WASHINGTON — In the closing days of 2015, the lights went out across a swath of Ukraine as Russian hackers remotely took over an electric utility's control center and flipped off one power station after another, while the company's operators stared at their screens helplessly.

The next year, the same thing happened, this time around Kyiv, the capital.

Now the United States and Britain have quietly dispatched cyberwarfare experts to Ukraine in hopes of better preparing the country to confront what they think may be the next move by President Vladimir V. Putin of Russia as he again menaces the former Soviet republic: Not an invasion with the 175,000 troops he is massing on the border, but cyberattacks that take down the electric grid, the banking system, and other critical components of Ukraine's economy and government.

Russia's goal, according to American intelligence assessments, would be to make Ukraine's president, Volodymyr Zelensky, look inept and defenseless — and perhaps provide an excuse for an invasion.

In one sense, the Russian cybercampaign against Ukraine never stopped, American officials say, though until recently it bubbled along at a low level. But in interviews, American officials and experts say the action has stepped up over the past month even while public attention has been focused on the troop buildup.

"It's a widespread campaign targeting numerous Ukrainian government agencies, including internal affairs — the national police — and their electric utilities," said Dmitri Alperovitch, a leading investigator of Russian cyberactivity and the chairman of Silverado Policy Accelerator, a new research group in Washington.

Mr. Alperovitch, who emigrated from Russia to the United States as a child, said the Russian leader sees the cyberattacks as “preparation of the battlefield.”

American officials say a military invasion is far from a certainty. “The current assessment of the U.S. government is that he has not made a decision,” said Jake Sullivan, President Biden’s national security adviser, speaking at the Council on Foreign Relations. Mr. Sullivan did not address the Russian cyberactivity, but it has been an intense focus at the White House, the C.I.A., the National Security Agency and United States Cyber Command, whose “cyber mission forces” are deployed to identify vulnerabilities around the world.

The Russian cyberactivity was discussed by roughly a dozen officials, who requested anonymity because the information was derived from classified intelligence and sensitive discussions about how to mitigate the Russian threat. Those conversations have focused on whether Mr. Putin thinks that a crippling of Ukraine’s infrastructure could be his best hope of achieving his primary goal: ousting the Ukrainian government and replacing it with a puppet leader.

The calculus, one senior intelligence official said, would be that such an attack would not require him to occupy the country — or suffer as many of the sanctions that would almost certainly follow a physical invasion.

Already Mr. Putin has been working to build support domestically and in Africa and South and Central America. Russian-led information campaigns have been focused on denigrating the Ukrainian government and accusing its leader of creating a humanitarian crisis in the country’s east, where Ukrainian government forces have been battling Russia-led separatists for years, according to U.S. and allied officials.

American officials declined to describe the cyberteams that have been inserted into Ukraine. In a statement, the Biden administration said only that “we have long supported Ukraine’s efforts to shore up cyberdefenses and increase its cyberresiliency.”

A spokeswoman for the British government said the assistance that Britain and its allies were providing was defensive in nature.

While neither government would provide details, officials said the United States was considering a larger deployment, including resources from U.S. Cyber Command. But it is unclear how much good a bigger team could do beyond demonstrating support.

“There’s too much to patch,” one American official said.

The Ukrainian grid was built in the days of the Soviet Union, connected to Russia’s. It has been upgraded with Russian parts. The software is as familiar to the attackers as to its operators. And while Ukraine has repeatedly vowed to fix its system, Mr. Putin’s hackers, or at least teams loyal to him, have shown time and time again that they know how to bring parts of the country to a halt.

In an interview, Sean Plankey, a former Energy Department cyberexpert who is now an executive at DataRobot, said that Russian hackers understand every linkage in the design — and most likely have insiders who can help them.

As the Ukrainians have learned, a cyberattack on critical infrastructure is particularly difficult to deter. In the cyberworld, there is no broad consensus about what constitutes an act of war, nor agreement about how deeply Mr. Putin could harm Ukraine without triggering a Western response. In the past, his attacks on Ukraine have resulted in almost no response.

The 2015 attack, which began in late December, was particularly instructive. It was directed at a major operator of Ukraine's grid. Videos taken during the attack showed a skeleton crew of operators — the attackers knew the holidays would be a particularly vulnerable time — struggling to understand what was happening as hackers took over their screens remotely. Substations were flipped off. Neighborhood by neighborhood, lights went dark.

"It was jaw-dropping for us," Andy Ozment, who ran cyberemergency response for the Department of Homeland Security and helped investigate the attacks, said at the time. "The exact scenario we were worried about wasn't paranoia. It was playing out before our eyes." The hackers had a final flourish: The last thing they turned off was the emergency power at the utility company's operations center, so that the Ukrainian workers were left sitting in their seats in the dark, cursing.

With the holidays approaching again, American officials say they are on high alert. But if Mr. Putin does launch a cyberattack, either as a stand-alone action or as a precursor to a physical-world attack, it will most likely come after Orthodox Christmas, at the end of the first week of January, according to people briefed on the intelligence.

Understand the Escalating Tensions Over Ukraine
Card 1 of 5
A brewing conflict. Antagonism between Ukraine and Russia has been simmering since 2014, when the Russian military crossed into Ukrainian territory, annexing Crimea and whipping up a rebellion in the east. A tenuous cease-fire was reached in 2015, but peace has been elusive.

A spike in hostilities. Russia has recently been building up forces near its border with Ukraine, and the Kremlin's rhetoric toward its neighbor has hardened. Concern grew in late October, when Ukraine used an armed drone to attack a howitzer operated by Russian-backed separatists.

Ominous warnings. Russia called the strike a destabilizing act that violated the cease-fire agreement, raising fears of a new intervention in Ukraine that could draw the United States and Europe into a new phase of the conflict.

The Kremlin's position. President Vladimir V. Putin of Russia, who has increasingly portrayed NATO's eastward expansion as an existential threat to his country, said that Moscow's military buildup was a response to Ukraine's deepening partnership with the alliance.

A measured approach. President Biden has said he is seeking a stable relationship with Russia. So far, his administration is focusing on maintaining a dialogue with Moscow, while seeking to develop deterrence measures in concert with European countries.

U.S. and allied officials have discussed a variety of sanctions that could possibly deter Russia. But all of the measures that could possibly cut deep enough for Russia to care would also cause pain in Europe, which is highly dependent on Russia for winter energy supplies.

Senator Angus King of Maine, a member of the Senate Intelligence Committee, said in an interview that if an invasion does take place, the first sign will be in cyberspace.

“I don’t think there’s a slightest doubt that if there is an invasion or other kind of incursion into Ukraine, it will start with cyber,” said Mr. King, an independent who caucuses with the Democrats.

Mr. King has long argued that the United States and its allies need to think more deeply about how to deter cyberattacks. The United States, Mr. King said, should issue a declaratory policy about what the consequences for such attacks will be.

“So the question is,” Mr. King said, “what are our tools to to deter that?”

Representative Mike Gallagher, Republican of Wisconsin who along with Mr. King leads the Cyberspace Solarium Commission, said the United States should try to prevent a cyberattack on Ukraine by making it clear it would prompt a strong response.

“We should be preparing our own cyberresponse,” Mr. Gallagher said. “We have very powerful weapons in the cyberdomain that we could use against Putin if he chooses to go further. We seem divided, but there’s a lot of options we have to prevent this from devolving into a full-on crisis.”

A cyberoperation retains allure for Moscow over a full-on military operation, because Russia can operate under a thin veil of deniability. And Mr. Putin has demonstrated over the last decade that the flimsiest of disguises is good enough.

In previous cyberattacks on Ukraine, Russian operatives made the incursions look like the work of criminal groups.

“After the fact, you can be pretty sure what we saw was state activity, using the false flag of criminal activity,” said Jim Richberg, the former national intelligence manager for cyber and now a vice president at Fortinet, a security firm. “They wanted it to have this broad impact on critical infrastructure in Ukraine and make it look like it was a criminal thing that went awry.”

For Mr. Putin, a cyberattack that he can officially deny, but no one doubts is his handiwork, is the best of both worlds.

“For someone like Putin, part of it is to be seen, to deliver a message,” Mr. Richberg said. “They can be good, but being good doesn’t mean they want to be invisible.”