Related news

cyberscoop.com/cybersecurity-experts-question-microsofts-ukraine-report

July 1, 2022

Cybersecurity experts question Microsoft's Ukraine report

Written by Suzanne Smalley
Jul 1, 2022 | CYBERSCOOP
Microsoft President Brad Smith spent much of last Wednesday traveling across Washington to promote his company's sweeping report on the current state of cyberwarfare and disinformation in the Russia-Ukraine war.

He sat down with David Ignatius, foreign affairs columnist for The Washington Post, for a webcast on its findings. Afterwards, he headed to the Reagan Institute's Center for Freedom and Democracy to give a 20-minute speech about the 27-page report called "Defending Ukraine: Early Lessons from the Cyber War" before joining Senator Angus King (I-ME) for a panel discussion.

The New York Times, CNN, The Washington Post, NPR and others covered the study as an accurate and revealing look at an otherwise opaque and confusing digital front in the Ukraine war.

Yet not long after the report surfaced, leading cybersecurity experts and foreign policy scholars began raising serious questions and concerns. They cast doubt on many of the key points of the document — namely claims about a combined physical and cyber attack on a nuclear power plant — and they complained that Microsoft is attempting to characterize the state of the cyber conflict in Ukraine to further its commercial interests.

"Microsoft is one of the most influential companies on the planet in this space [and] Microsoft has a responsibility to get this right," said Thomas Rid, a cybersecurity scholar and Johns Hopkins University School of Advanced International Studies professor. "If you publish this kind of information, you have to do it in a way that is sober, in a way that is fact driven, and in a way that uses professional estimative language."

In total, CyberScoop spoke with a dozen prominent cybersecurity threat analysts, executives, military cyber practitioners and scholars who all criticized Microsoft for publishing a report that didn't contain either the technical underpinning or evidence to back up its points. What's more, they said, it didn't meet basic standards of academic research that even most tech companies adhere to when producing similar reports on nation-state or criminal cyber threat activities.

Little sourcing, big claims

"Source citations are thin to nonexistent," said Christopher Paul, a disinformation researcher and senior social scientist at RAND Corporation. There's a "smattering of links in text to specific sources and other reporting, and the first actual reference being a figure source for a copy of a newspaper page from the '80s," he said. Paul also noted that the report sourced many figures and tables to Microsoft's own AI for Good Research Lab — a group that Microsoft calls a "philanthropic team of data scientists and researchers" who focus on artificial intelligence and machine learning — without enough further detail.

Microsoft does have unique insight into cyberattacks carried out in Ukraine, and, for that matter, much of the world, as one of the biggest global technology companies. It also often works with the U.S. government on cybersecurity operations due to the reach and scale of its networks. It stands to reason that it would be positioned to understand the nature of the cyber conflict in Ukraine and help inform the public, policymakers and experts in the field.

> "If you publish this kind of information, you have to do it in a way that is sober, in a way that is fact driven, and in a way that uses professional estimated language."
>
> *thomas rid, cybersecurity scholar*

Likewise, CyberScoop and many other publications regularly cover industry reports on cyber activities and nation-state operatives. But in this case, experts say, Microsoft's powerful global market position, the potential commercial benefits from positioning itself as a bulwark against Russian cyberattacks and the extremely delicate situation in Ukraine make this report's bold claims and lack of data concerning.

To be sure, much remains unknown about the contours of cyber warfare in Ukraine and all of the ways in which Russia is using cyber means as part of its brutal campaign. But many of the critics took issue with the report because they believe it overstates the degree to which Russia has coordinated cyber and physical warfare and feel that it portrays Russia's operations in Ukraine as overly sophisticated.

In a statement to CyberScoop, a Microsoft spokesperson defended the report and disputed the characterizations from critics, saying the company wanted to reach a broader audience that may not be well versed in the technical nature of cyberattacks.

"Cybersecurity issues are pervasive across the digital landscape, extending beyond the security community to key audiences including policymakers and others not always steeped in technical details," the spokesperson said. "We stand by our report and its findings and welcome an ongoing conversation with others in the security community and beyond as we work together to do our part to defend Ukraine and protect the cybersecurity ecosystem."

Questions about an alleged nuclear power plant assault

The main objection from many experts involves unsubstantiated claims that Microsoft made about an apparent assault on a Ukrainian power plant that allegedly combined a physical strike with a cyberattack.

The report said the "Russian military combined cyber and conventional weapons in assaulting a nuclear power plant" in early March, pointing to a Russian group moving laterally on the nuclear power company's computer network on March 2 before a military attack on March 3.

Most of the dozen experts CyberScoop spoke with called this assertion deeply problematic. Rid points out that while Microsoft initially implied the Russians used cyber to collect intelligence from the nuclear power plant, in the following sentence the report appears to hedge, saying the highly regarded Microsoft Threat Intelligence Center (MSTIC) "identified a Russian group moving laterally on the nuclear power company's computer network."

"This [statement] is full of assumptions," said Rid, who has written extensively on Russian intelligence and who said changing the focus from the plant itself to the larger company is misleading. "The first sentence is not backed up by the second."

He also pointed out that while the report called the cyber incident at the plant a "weapon" the description of the Russian group "moving laterally" does not qualify as a weapon.

Rid said that despite his view of the Microsoft report on Ukraine, typically the work that comes from MSTIC is high caliber and presented without the sheen of corporate marketing or grandstanding. "I have the highest respect for MSTIC and the forensic and investigative work they have been doing — this report, strangely, does not reflect the quality of their work," he said.

Another noted cybersecurity expert, Juan Andres Guerrero-Saade, also said the nuclear plant anecdote appears to overestimate the current strategic capabilities of the Russian military.

“It’s incredibly charitable to suggest that the reality of the Russian military is one that includes organized coordination between different intelligence units and kinetic forces,” said Guerrero-Saade, principal threat researcher at SentinelOne and an adjunct professor at SAIS. “It builds a view of a formidable bear that we haven’t quite seen.”

(SentinelOne is a competitor of Microsoft Defender for Endpoint, a security platform that helps defend against advanced persistent threats).

Understanding the stakes

Due to the current situation in Ukraine and the policy questions which it raises, it’s more important than ever to get the facts straight about what may or may not be happening on the ground or in the digital realm, Guerrero-Saade said.

“At a time when there are suggestions to include cyber as a domain that the International Criminal Court should consider as part of war crimes investigations, research teams and technical output should be kept as objective and rigorous as possible,” he said.

The nuclear power plant story caught the attention of a senior defense official, too.

“In terms of a cyberattack, strategically that is something that the Russians do not want to do,” Ryan Maness, the Defense Analysis Department Director at the Naval Postgraduate School and the author of “Cyber War Versus Cyber Realities: Cyber Conflict in the International System,” said via email from Europe. “They wanted the plant intact for a strategic energy advantage against Ukraine (blackmail, coercion), so they wanted it in working order. The shooting around the plant was irresponsible, yes, but as far as I know, was not threatening to the reactors.”

Microsoft is presenting a “very incomplete assessment of the cyber situation of the war,” he said.

Like others who spoke with CyberScoop, Maness said the report gives the Russians too much credit.

Many of the document’s most outspoken critics said that a report of this magnitude should have read less like a marketing pitch for Microsoft and relied more on indicators of compromise and sober technical analysis. Instead, Guerrero-Saade said, the report appears to be an “attempt to take technical research and turn it into a strange lobbying opportunity.”

Guerrero-Saade also said the report too often makes claims that are questionable. For instance, he said, the report makes connections between specific cyber threats and individual Russian intelligence agencies without evidence to support those links. Specifically, the report attributes various phishing, data theft and wiper attacks to three different Russian intelligence agencies without explaining how it is making each attribution. He said such links are typically difficult for even the best threat analysts to establish.

Michael van Landingham, who was a Russia analyst for the CIA until 2019 and who now runs Actives Measures, a research and analysis firm, also said the report’s lack of data undermines its findings. For example, he said, it was unclear how Microsoft determined that only 29 percent of Russia’s attempted cyber intrusions aimed at Ukraine succeeded.

“What is the scope of Russian cyber activity that you’re catching as Microsoft, with your data, or that you’re measuring, and what might you be missing?” he said. “I want to see more discussion of what Microsoft can see and what they can’t see, and how that affects their confidence levels in their judgments about stopping intrusions

and also breaking out what the threat intelligence team or what the authors think broadly these intrusions were for."

Overall, he said, he worries that the report's generalizations leave a nontechnical audience with more questions than answers.

"When you're writing for a broader audience, all of those things get lumped into the big CYBER!," he said. "But the problem with the CYBER! is that [reality] is obviously much more nuanced and not everything under that umbrella of CYBER! has the same impact in an armed conflict as the authors or a generalist audience might expect."