Think Tank: Cyber Firm at Center of Russian Hacking Charges Misread Data

Last Updated: March 23, 2017 11:17 AM

Oleksiy Kuzmenko Pete Cobus

WASHINGTON —

An influential British think tank and Ukraine’s military are disputing a report that the U.S. cybersecurity firm CrowdStrike has used to buttress its claims of Russian hacking in the presidential election.

The CrowdStrike report, released in December, asserted that Russians hacked into a Ukrainian artillery app, resulting in heavy losses of howitzers in Ukraine’s war with Russian-backed separatists.

But the International Institute for Strategic Studies (IISS) told VOA that CrowdStrike erroneously used IISS data as proof of the intrusion. IISS disavowed any connection to the CrowdStrike report. Ukraine’s Ministry of Defense also has claimed combat losses and hacking never happened.

A CrowdStrike spokesperson told VOA that it stands by its findings, which, they say, "have been confirmed by others in the cybersecurity community.”

The challenges to CrowdStrike’s credibility are significant because the firm was the first to link last year’s hacks of Democratic Party computers to Russian actors, and because CrowdStrike co-founder Dimiti Alperovitch has trumpeted its Ukraine report as more evidence of Russian election tampering.

Alperovitch has said that variants of the same software were used in both hacks.

FILE - CrowdStrike co-founder and CTO Dmitri Alperovitch speaks during the Reuters Media and Technology Summit in New York, June 11, 2012.

FILE - CrowdStrike co-founder and CTO Dmitri Alperovitch speaks during the Reuters Media and Technology Summit in New York, June 11, 2012.

While questions about CrowdStrike’s findings don’t disprove allegations of Russian involvement, they do add to skepticism voiced by some cybersecurity experts and commentators about the quality of their technical evidence.

The Russian government has denied covert involvement in the election, but U.S. intelligence agencies have concluded that Russian hacks were meant to discredit Hillary Clinton and help Donald Trump’s campaign. An FBI and Homeland Security report also blamed Russian intelligence services.

On Monday, FBI Director James Comey confirmed at a House Intelligence Committee hearing that his agency has an ongoing investigation into the hacks of Democratic campaign computers and into contacts between Russian operatives and Trump campaign associates. The White House says there was no collusion with Russia, and other U.S. officials have said they’ve found no proof.

Signature malware

VOA News first reported in December that sources close to the Ukraine military and the artillery app’s creator questioned CrowdStrike’s finding that a Russian-linked group it named “Fancy Bear” had hacked the app. CrowdStrike said it found a variant of the same “X-Agent” malware used to attack the Democrats.

FBI Director James Comey, left, and National Security Agency Director Mike Rogers during the House Permanent Select Committee on Intelligence hearing on Russian actions during the 2016 election campaign, March 20, 2017.

FBI Director James Comey, left, and National Security Agency Director Mike Rogers during the House Permanent Select Committee on Intelligence hearing on Russian actions during the 2016 election campaign, March 20, 2017.

CrowdStrike said the hack allowed Ukraine’s enemies to locate its artillery units. As proof of its effectiveness, the report referenced publicly reported data in which IISS had sharply reduced its estimates of Ukrainian artillery assets. IISS, based in London, publishes a highly regarded, annual reference called “The Military Balance” that estimates the strength of world armed forces.

“Between July and August 2014, Russian-backed forces launched some of the most-decisive attacks against Ukrainian forces, resulting in significant loss of life, weaponry and territory,” CrowdStrike wrote in its report, explaining that the hack compromised an app used to aim Soviet-era D-30 howitzers.

“Ukrainian artillery forces have lost over 50% of their weapons in the two years of conflict and over 80% of D-30 howitzers, the highest percentage of loss of any other artillery pieces in Ukraine’s arsenal,” the report said, crediting a Russian blogger who had cited figures from IISS.

The report prompted skepticism in Ukraine.

Yaroslav Sherstyuk, maker of the Ukrainian military app in question, called the company’s report “delusional” in a Facebook post. CrowdStrike never contacted him before or after its report was published, he told VOA.

Pavlo Narozhnyy, a technical adviser to Ukraine’s military, told VOA that while it was theoretically possible the howitzer app could have been compromised, any infection would have been spotted. “I personally know hundreds of gunmen in the war zone,” Narozhnyy told VOA in December. “None of them told me of D-30 losses caused by hacking or any other reason.”

VOA first contacted IISS in February to verify the alleged artillery losses. Officials there initially were unaware of the CrowdStrike assertions. After investigating, they determined that CrowdStrike misinterpreted their data and hadn’t reached out beforehand for comment or clarification.

In a statement to VOA, the institute flatly rejected the assertion of artillery combat losses.

“The CrowdStrike report uses our data, but the inferences and analysis drawn from that data belong solely to the report's authors,” the IISS said. “The inference they make that reductions in Ukrainian D-30 artillery holdings between 2013 and 2016 were primarily the result of combat losses is not a conclusion that we have ever suggested ourselves, nor one we believe to be accurate.”

One of the IISS researchers who produced the data said that while the think tank had dramatically lowered its estimates of Ukrainian artillery assets and howitzers in 2013, it did so as part of a “reassessment” and reallocation of units to airborne forces.

"No, we have never attributed this reduction to combat losses," the IISS researcher said, explaining that most of the reallocation occurred prior to the two-year period that CrowdStrike cites in its report.

“The vast majority of the reduction actually occurs ... before Crimea/Donbass,” he added, referring to the 2014 Russian invasion of Ukraine.

‘Evidence flimsy'

In early January, the Ukrainian Ministry of Defense issued a statement saying artillery losses from the ongoing fighting with separatists are “several times smaller than the number reported by [CrowdStrike] and are not associated with the specified cause” of Russian hacking.

But Ukraine’s denial did not get the same attention as CrowdStrike’s report. Its release was widely covered by news media reports as further evidence of Russian hacking in the U.S. election.

In interviews, Alperovitch helped foster that impression by connecting the Ukraine and Democratic campaign hacks, which CrowdStrike said involved the same Russian-linked hacking group—Fancy Bear—and versions of X-Agent malware the group was known to use.

“The fact that they would be tracking and helping the Russian military kill Ukrainian army personnel in eastern Ukraine and also intervening in the U.S. election is quite chilling,” Alperovitch said in a December 22 story by The Washington Post.

The same day, Alperovitch told the PBS NewsHour: “And when you think about, well, who would be interested in targeting Ukraine artillerymen in eastern Ukraine? Who has interest in hacking the Democratic Party? [The] Russia government comes to mind, but specifically, [it's the] Russian military that would have operational [control] over forces in the Ukraine and would target these artillerymen.”

Alperovitch, a Russian expatriate and senior fellow at the Atlantic Council policy research center in Washington, co-founded CrowdStrike in 2011. The firm has employed two former FBI heavyweights: Shawn Henry, who oversaw global cyber investigations at the agency, and Steven Chabinsky, who was the agency's top cyber lawyer and served on an Obama White House cybersecurity commission in 2016. Chabinsky left CrowdStrike last year.

CrowdStrike declined to answer VOA’s written questions about the Ukraine report, and Alperovitch canceled a March 15 interview on the topic. In a December statement to VOA’s Ukrainian Service, spokeswoman Ilina Dimitrova defended the company’s conclusions.

“It is indisputable that the [Ukraine artillery] app has been hacked by Fancy Bear malware,” Dimitrova wrote. “We have published the indicators to it, and they have been confirmed by others in the cybersecurity community.”

In its report last June attributing the Democratic hacks, CrowdStrike said it was long familiar with the methods used by Fancy Bear and another group with ties to Russian intelligence nicknamed Cozy Bear. Soon after, U.S. cybersecurity firms Fidelis and Mandiant endorsed CrowdStrike’s conclusions. The FBI and Homeland Security report reached the same conclusion about the two groups.

Still, some cybersecurity experts are skeptical that the election and purported Ukraine hacks are connected. Among them is Jeffrey Carr, a cyberwarfare consultant who has lectured at the U.S. Army War College, the Defense Intelligence Agency, and other government agencies.

In a January post on LinkedIn, Carr called CrowdStrike’s evidence in the Ukraine “flimsy.” He told VOA in an interview that CrowdStrike mistakenly assumed that the X-Agent malware employed in the hacks was a reliable fingerprint for Russian actors.

“We now know that’s false,” he said, “and that the source code has been obtained by others outside of Russia."

This report was produced in collaboration with VOA's Ukrainian Service.