US retaliated against Iranian spy group's cyberstrike

By Kylie Atwood and Caroline Kelly, CNN

Updated 0506 GMT (1306 HKT) June 23, 2019

(CNN) — US Cyber Command launched a retaliatory cyberstrike last week against an Iranian spy group, according to a US official and a former US intelligence official familiar with the matter.

USCC attacked the spy group, which has ties to the Islamic Revolutionary Guard Corps, after Iran attacked ships in the region, the officials said.

The US official added the online strike targeted an Iranian spy group's computer software that was used to track the tankers that were targeted in the Gulf of Oman on June 13.

A spokesman for the Pentagon would not comment on the matter Saturday, saying that "as a matter of policy and for operational security, we do not discuss cyberspace operations, intelligence or planning."

Yahoo! News first reported the US cyberstrike against Iran.

The exchanged attacks come following a tumultuous week between the two countries. Iran shot down an American drone Thursday, prompting President Donald Trump to pursue a retaliatory strike against Iran.

Trump said Friday that he called off the attack on Iran -- with the US "cocked & loaded"-- 10 minutes before the strike because he decided there would be too many deaths for a proportionate response to the downing of an American drone. He claimed Saturday that he is "getting a lot of praise" for his abrupt decision to reverse course.

The former US intelligence official told CNN that in recent months there has been an increase in Iranian cyber activity against Gulf targets, like Bahrain and the United Arab Emirates, as well as US targets. Iranian forces' cyber capabilities have improved in recent years, and while they often outsource their efforts to Russians, it is expected that the Iranians carried out this attack themselves.

The Department of Homeland Security announced Saturday that Iran has recently increased cyberattacks against US industry and government agencies as tension peaked between the countries this week.

Christopher Krebs, the director of DHS's Cybersecurity and Infrastructure Security Agency, said in a statement that his agency "is aware of a recent rise in malicious cyber activity directed at United States industries and government agencies by Iranian regime actors and proxies."

"We will continue to work with our intelligence community and cybersecurity partners to monitor Iranian cyber activity, share information, and take steps to keep America and our allies safe," he added.

Krebs said Iranian state actors and proxies are increasingly using "destructive 'wiper' attacks" that are capable of not only stealing data and money but taking down an organization's entire computer network.

CNN's Ryan Browne, David Shortell and Geneva Sands contributed to this report.