U.S. Cyber Command back in the Headlines

05/07/2019



Although the United States Cyber Command (USCYBERCOM) mission was top secret at first, it has gradually become crystal clear.

Its operations, surrounded by mystery for over a decade, are back in the headlines. According to press reports, after the downing of a U.S. drone last Thursday and the subsequent last-minute cancellation of airstrikes against Iranian's military targets by Trump, the USCYBERCOM elite forces stroke back with a computer virus attack.

According to AP, the computer virus attack targets military objectives and "was a demonstration of the U.S.'s increasingly mature cyber military capabilities and its more aggressive cyber strategy under the Trump administration. Over the last year U.S. officials have focused on persistently engaging with adversaries in cyberspace and undertaking more offensive operations."

In the same way, the ***New York Times*** released this month a news article where it was confirmed that Washington tried to sabotage Russia's power grid and insert some computer viruses to activate them in case of conflict, or signs of a new Kremlin's meddling in the U.S. internal affairs.

The ***BBC*** affirms that the USCYBERCOM is a virtual army, a new type of weaponry, a never seen before fight machinery.

The article adds that such elite unit of the Pentagon is responsible for defending the country and attacking its enemies in a war zone made up of codes and bits since 2009. The Cyber Command is one of the 10 combatant commands of the DoD (Department of Defense).

In the view of Michael Warner, USCYBERCOM historian who was quoted by the ***BBC***, the creation of USCYBERCOM marked the culmination of more than a decade's worth of institutional change and was then nominated as a special unit working in collaboration with National Security Agency (NSA) sharing its headquarter in Fort Meade, Maryland.

In 2017, the Pentagon decided to appoint USCYBERCOM as a "combatant command" and suggested the possibility of separating it from the NSA. A year later, the unit culminated the process of creation of its Cyber Combat Mission Force, which gathered nearly 6,200 soldiers organized in 133 teams.

"The Cyber Command is responsible for carrying out operations in the military computer network whereas the NSA is responsible for cyber espionage," pointed out Max Smeets — cybersecurity investigator at Stanford University Center for International Security and Cooperation (CISAC).

According to its website, the Cyber Command not only "leads operations and defends the U.S. networks." But they also, "at the appropriate time," look to "engage in military operations in the cyberspace" to guarantee the freedom of action of the U.S. and its allies" while "preventing the enemy to do the same."

Moreover, Smeets believes that even though military cyber organizations (units, services, commands) operate under different legal, political, and operational restrictions, most of them lead a very specific operation:

"Causing a specific cyber effect, targeting, in a certain given period of time; with a strategic mission and overcoming other possible negative implications."

Michael Ahern, Director of Power System at the Worcester's Polytechnic Institute, told ***BBC Mundo*** thatthe security of electricity grids has become a concern for many nations,not only because of the possibility of "terrorist" attacks ", but also by "enemy" governments.

He explained that "as modern societies become more and more dependent on computers and the exchange of data through the Internet, they have also become more vulnerable to cyber threats.

"Hence, a cyber-attack may potentially damage water pumping stations and other services of critical need can have more devastating effects than weapons in conventional wars.

"That is why it is likely that all nations are working to improve their cybernetic capabilities There have been a couple of attacks that caused power cuts in Ukraine, and in North America, the Federal Energy Regulatory Commission requires network operators that comply with a critical infrastructure protection plan," he pointed out.

In March, Venezuela suffered a cyber-attack leaving the country in the dark. Venezuela's President Nicolas Maduro denounced back then that "the sabotage against the power grip was carried out in order to trigger civil outrage aiming at undermining the political power" had been ordered by the U.S. Southern Command and staged from Houston and Chicago, two American

cities.

According to experts quoted by the ***BBC***, the USCYBERCOM has drastically grown in the last decade. Hence, its budget, workforce and operational range have multiplied considerably. The budget allocated by the government to this unit —US$120 in 2010— topped US$600 in 2018.

From June 2018 on, the Pentagon has granted even further authority to USCYBERCOM to implement more aggressive campaigns. Under the auspice of the 2018 National Defense Authorization Act, the USCYBERCOM is allowed to “carry out clandestine military activities” in the network without seeking the President’s clearance.

Translated by Sergio A. Paneque Díaz/CubaSí Translation Staff