US's strategy to defeat ISIS by carrying cyber war and dropping cyber bombs

US had devised a new strategy to defeat ISIS, and also started cyber warfare campaign against ISIS. US is first in world to have publically declare that it is carrying cyber war against ISIS that involves dropping "cyber bombs"-the term coined by Ash carter- to disrupt its communications and other infrastructure. The cyber warfare campaign is being carried out by military's seven-year-old U.S. Cyber Command through full range of cyber warfare methods.

A new unit headed by Lt. Gen. Edward Cardon was tasked with developing digital weapons – fashioned from malware and other cyber-tools – that can intensify efforts to damage and destroy the Islamic State's networks, computers and cellphones. This was also a test of operational effectiveness of its cyber command to conduct offensive mission against ISIS that was formed to thwart traditional foes like Russia, China, Iran and North Korea. The terror groups like ISIS use social media platforms like Twitter, Facebook, YouTube and internet forums to spread their messages, recruit members and gather intelligence.

While U.S. Cyber Command claimed success in carrying out what was called Operation Glowing Symphony, under which Cyber Command obtained the passwords to a number of Islamic State administrator accounts and then used them to access the accounts, change the passwords and delete content such as battlefield video. It also shut the group's propaganda specialists out of their accounts, former officials said.

However, Last year, then-Defense Secretary Ash Carter expressed frustration that the United States was losing the

cyberwar against the militants. He pushed the Cyber Command to be more aggressive. In response, the Pentagon undertook an effort to incorporate cyber technology into its daily military fight, including new ways to disrupt the enemy's communications, recruiting, fundraising and propaganda.

The military is now looking for new ways to bring in more civilians with high-tech skills who can help against IS and prepare for the new range of technological threats the nation will face, as reported by AP. Lt. Gen. Paul Nakasone commander of U.S. Army Cyber Command said that means getting Guard and Reserve members with technical expertise in digital forensics, math crypto-analysis and writing computer code. According to Nakasone they are bringing new expertise for identifying enemy networks, pinpointing system administrators or developers, and potentially monitoring how IS' online traffic moves.

The Army has been steadily building cyber mission teams, as part of a broader Defense Department undertaking. Of the 41 Army teams, just over half come from the Army National Guard and Army Reserve.

United States opened a new line of combat against the Islamic State, directing the military's eight-year-old Cyber Command for the first time to mount computer-network attacks that are now being used alongside more traditional weapons. In 2009, US established, USCYBERCOM for more effective and coordinated efforts for conducting cyberspace operations. Cyber Command, which was focused largely on Russia, China, Iran and North Korea – where cyberattacks on the United States most frequently originate – has now been given responsibility for operations against what has become the most dangerous terrorist organization in the world.

To know more about USAF cyber platforms :http://idstch.com/home5/international-defence-sec

urity-and-technology/cyber/usaf-offensive-cyberspace-operations-oco-program-developing-cyber-mission-platforms-cyber-weapons-platform-command-control-mission-system/

"The cyberwar seal has been broken in public", said Peter W Singer of the New America Foundation. In addition to overloading or defacing Isis's web presence, known as a denial of service attack, and aiming to prevent the uploading or distribution of propaganda, particularly on social media, it is likely that the US Cyber Command is "mapping the people behind networks, their connections and physical locations and then feeding that into targeting on the kinetic side – injecting false info to create uncertainty", Singer said.

However, a report by The Washington Post said that militant group's "sophisticated" use of technology is making it difficult for the Pentagon to disrupt the group's operations and spread of propaganda with specially-crafted malware designed to target the group's computers, mobile devices, and infrastructure. "Cybercom has not been as effective as the department would expect them to be, and they're not as effective as they need to be," said a senior defense official who, like other officials, spoke on the condition of anonymity to discuss internal conversations. "They need to deliver results."

The situation is difficult as the ISIS is having decentralized architecture which is constantly moving instead of government or nation-state, which relies on fixed and traditional infrastructure. This complicates the targeting as cybercom has to target individuals with malware or long range jamming which may have an adverse effect on civilians. Terrorist's use of encryption is also hampering operations.

"The more dependent you are on technology, the more you are a target for cyberattack. And ISIS is less dependent," said James Lewis, a cyber-policy expert at the Center for Strategic

and International Studies, as reported by The Washington Post.

Disrupting ISIS's Command and Control and communications

"Our cyberoperations are disrupting their command-and-control and communications," Mr. Obama said this month, emerging from a meeting at the C.I.A. headquarters in Langley, Va., on countering the Islamic State.

While officials declined to discuss the details of their operations, interviews with more than a half-dozen senior and midlevel officials indicate that the effort has begun with a series of "implants" in the militants' networks to learn the online habits of commanders. Now, the plan is to imitate them or to alter their messages, with the aim of redirecting militants to areas more vulnerable to attack by American drones or local ground forces.

Earlier, US Defense Secretary Ashton Carter had said the cyber effort was focused primarily on ISIS terrorists in Syria and that the campaign's goal was to "overload their network so that they can't function" and "interrupt their ability to command and control forces there, control the population and the economy."

"US's deterrence strategy, which by definition is based on the threat of consequences, is unlikely to succeed in the fight against ISIS or similarly minded groups. Death is a goal for many jihadists, and one to be celebrated." With few deterrent options, the United States and its partners should support efforts aimed at dissuading would-be fighters before they make the decision to join ISIS, says Thomas M. Sanderson

Cyber Warfare also to counter ISIS propaganda and collect intelligence

The goal of the new campaign is to disrupt the ability of the Islamic State to spread its message, attract new adherents, circulate orders from commanders and carry out day-to-day functions, like paying its fighters. A benefit of the administration's exceedingly rare public discussion of the campaign, officials said, is to rattle the Islamic State's commanders, who have begun to realize that sophisticated hacking efforts are manipulating their data. Potential recruits may also be deterred if they come to worry about the security of their communications with the militant group.

The U.S. efforts to monitor ISIS's use of social media and counter its online propaganda and recruitment efforts have been tentative, hesitant and amateurish. Responsibility for counter-messaging has shifted between various organizations, but these agencies do not seem to share lessons learned or even operate using a cohesive strategy, write ANDREW BYERS AND TARA MOONEY in The HILL. They suggest bringing together small teams of counterterrorist experts; regional experts who know the languages, dialects, actors and groups involved; and social media-savvy technical experts is a cheap and cost-effective approach.

Terrorism expert Sidney Jones said the country needed a cyber defense agency in order to analyze cyberspace traffic on the Internet, on social media and also on messenger services.

Goals and objectives

Mr Carter has said that by disrupting ISIS' communications,

these cyberattacks risked hindering US intelligence collection. But he said that such “trade-offs” did not detract from the need to disrupt ISIS’ networks.

Carter and the chairman of the Joint Chiefs of Staff, Marine Gen Joseph Dunford, declined to speak about the US cyber campaign in detail, but said it contributed the broader objectives of isolating the Isis capital of Mosul in Iraq and Raqqa in Syria.

Article sources also include:

http://csis.org/files/publication/141117_Sanderson.pdf

http://www.militarytimes.com/story/military/war-on-is/2016/01/14/pentagon-strategy-islamic-state-iraq-syria/78269180/

https://www.washingtonpost.com/world/national-security/us-militarys-digital-war-against-the-islamic-state-is-off-to-a-slow-start/2016/07/15/76a3fe82-3da3-11e6-a66f-aa6c1883b6b1_story.html

https://www.yahoo.com/tech/army-taps-reservists-cyber-skills-fight-militants-063211345.html

http://thehill.com/blogs/pundits-blog/defense/325082-isis-is-winning-the-cyber-war-heres-how-to-stop-it