(Video) Threat From Iranian Regime's Cyber Army Is Real but Over-sold

In recent years, social media networks have become very popular among Iranians, and so authorities have been bending over backward to control these platforms.

Hossein Salami,"We have 2,000 organized and active cyber battalions. The situation has improved regarding content creators, operations, and infrastructure," Salami bragged in remarks quoted by the state-run Hamshahri online on September 6.

PARIS, FRANCE, September 11, 2022 /EINPresswire.com/ -- Hossein Salami, the commander of Iran's Islamic Revolutionary Guard Corps (IRGC), delivered a boastful speech on Tuesday in which he claimed that the internationally-recognized terrorist organization has a "2,000-battalions strong cyber army."

"We have 2,000 organized and active cyber battalions. The situation has improved regarding content creators, operations, and infrastructure," Salami bragged in remarks quoted by the state-run Hamshahri online on September 6.

> On December 10, 2020, Treadstone 71, LLC, a California-based cyber intelligence and counterintelligence company, released details of an Iranian intelligence-backed influence operation."
>
> *NCRI*

Salami also called for activating what he described as a "national intelligence network," or simply making Iran's cyberspace like North Korea's and controlling information flow.

In recent years, social media networks have become very popular among Iranians, and so authorities have been bending over backward to control these platforms.

Salami's speech was not the only instance of Iranian officials promoting the concept of "cyber army power." In November 2021, Gholamreza Soleimani, the head of the IRGC's Basij Organization, announced the launch of nearly 3,500 cyber battalions.

And in March 2022, a former head of the Culture Ministry's Digital Media Center explained how some of its online disinformation programs operate.

"We created new accounts on Twitter, using the persona of other Twitter influencers who were mainly counter-revolutionary activists. Ours just differed in a single character and was quite similar to the real one.

We used the same picture and the same name, but everything was fake. Once created, we started our activities," said Ruhollah Momen Nasab, who now oversees the parliamentary bill to restrict Iran's internet, in an interview with state TV.

Tehran has been investing in its cyber power in recent years to target its adversaries abroad and to increase domestic surveillance, while activists have used social media networks to coordinate anti-regime protests. Tehran also uses its cyber army as a coercive tool and to extract confessions from world powers.

Salami's speech was not the only instance of Iranian officials promoting the concept of "cyber army power." In November 2021, Gholamreza Soleimani, the head of the IRGC's Basij Organization, announced the launch of nearly 3,500 cyber battalions.

Ruhollah Mo'men Nasab, special advisor "We created new accounts on Twitter, using the persona of other Twitter influencers who were mainly counter-revolutionary activists. Ours just differed in a single character and was quite similar to the real one.

According to a report by the Center for Strategic and International Studies on June 25, 2019, three military organizations were then playing leading roles in cyber operations: the Iranian Revolutionary Guard Corps (IRGC), the Basij, and Iran's 'Passive Defense Organization (NPDO).'"

On September 7, 2022, Mandiant Intelligence published a report about the destructive activities of the APT42 hacking group. The report described APT42 as "an Iranian state-sponsored cyber espionage group tasked with conducting information collection and surveillance operations against individuals and organizations of strategic interest to the Iranian government.

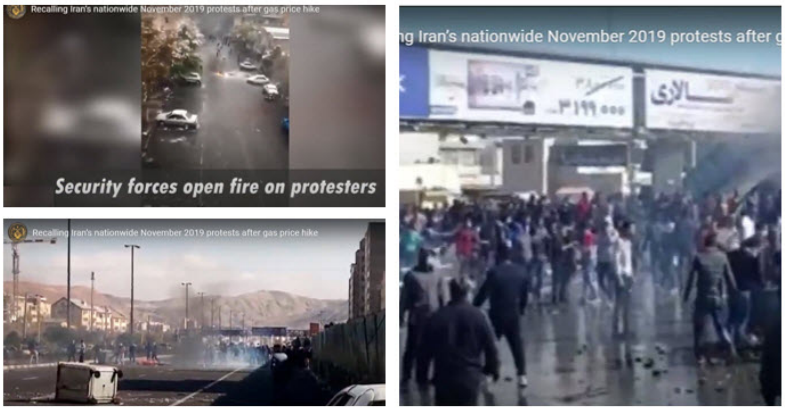
In a comprehensive report in April, the Iranian Resistance revealed damning information about

the Iranian regime's so-called cyber army and how it operates. This report highlighted how Tehran's "cyber-army generates multiple accounts that support each other to maximize propaganda circulation."
"The fake accounts regularly pose as anti-regime figures, such as Maryam Rajavi, Massoud Rajavi... or even media outlets like the BBC and Iran International," the report added.

In its study, 'How the IRGC Uses Cyberwarfare to Preserve the Theocracy,' the National Council of Resistance of Iran (NCRI)'s Washington office provided evidence about how Tehran has been using its cyber army to flood the internet with misinformation, paving the way for cracking down on popular uprisings.

On December 10, 2020, Treadstone 71, LLC, a California-based cyber intelligence and counterintelligence company, released details of an Iranian intelligence-backed influence operation.

Unlike what Salami and other officials try to sell, Tehran's development of cyber power is a reaction to its vulnerabilities. If the regime enjoys domestic & international legitimacy, why does it have to create fake accounts to hack infrastructures abroad?



The nationwide boycott of Iran's sham presidential elections in recent years, ongoing protests by people from all walks of life, and eight major uprisings in less than six years indicate that the ruling theocracy faces a crisis of illegitimacy.

"The IRGC, MOIS, and low-level Basij Cyber Units flooded Twitter with nearly one hundred twelve thousand tweets over sixty hours using hashtags and content intent on controlling the social media narrative," read the report.

Unlike the narrative Salami and other officials try to sell, Tehran's development of cyber power is a reaction to its vulnerabilities. If the clerical regime enjoys domestic and international legitimacy, why does it have to create fake accounts to target dissidents or hack infrastructures abroad?

Salami answered this question in his speech on Tuesday: "The enemy seeks to dominate cyberspace and twist the truth. Cyberspace has become the enemy's most dangerous field of operation."

The nationwide boycott of Iran’s sham presidential and parliamentary elections in recent years, ongoing protests by people from all walks of life, and eight major uprisings in less than six years indicate that the ruling theocracy faces a crisis of illegitimacy.

Social media networks have played a major role in the organization of recent protests.

It is safe to say that the Iranian regime’s efforts to strengthen its cyber-army are a sign of weakness, but its threat should be taken seriously. Western powers should make concerted efforts to undermine Tehran’s malicious attacks and address their potential to wreak havoc worldwide.

Shahin Gobadi
NCRI
+33 6 61 65 32 31
email us here