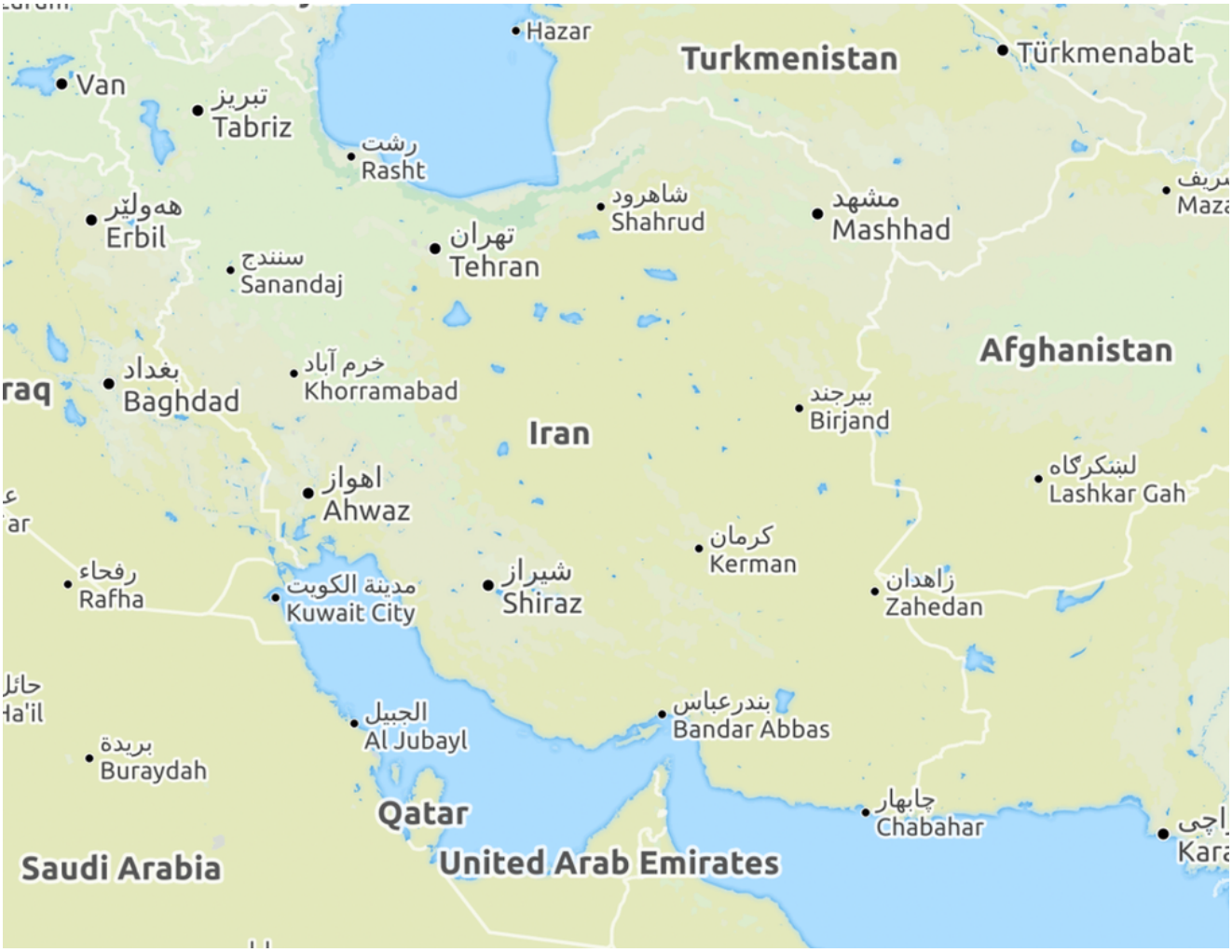
Iran’s Cyber Campaign, and Coercive Recruitment Methods

mideastcenter.org/post/iran-s-cyber-campaign-and-coercive-recruitment-methods

MECRA January 16, 2021



- MECRA
-
-
  - Jan 16, 2021
  -
  - 7 min read

Regime recruits hackers by coercion

A number of Iranian IRGC-related computer hackers are currently on the FBI wanted list. Evidence is emerging, however, that some Iranian hackers, participants in Iran's cyber sabotage operations against foreign governments, have been coerced into taking part in these operations. MECRA's Iran correspondent investigated this issue.

'Ali' (not his real name) is a computer programmer and is one of the hackers on the FBI wanted list. A friend of his, in conversation with MECRA, gave the following testimony:

"Ali was forced to cooperate. They made a trap for him. Very few of his friends know that he is a homosexual. In a religious city with his religious family, it would be a major disaster for him and his family if people knew about this

Ali was contacted by an anonymous person who sent him an excerpt from a recorded video showing him having sexual relations with another man, and threatening to publish the video. Over a period of weeks, Ali was sent additional excerpts from the same individual. At first, Ali was convinced that the anonymous caller was his former partner. He contacted his former partner, who denied any involvement.

After a month, Ali received a call from a number, which invited him to come in for a meeting. He realized that the number was from the Ministry of Intelligence. He attended the meeting. Initially, his questioners asked him about his online private customers and activities. They explained that they were concerned because of the recent hacking of an Iranian bank. In a subsequent meeting, Ali was then asked to cooperate with the ministry's team of hackers in attacking anti-government sites.

These were websites of political groups located outside of Iran. Ali agreed to become involved with the project. The ministry then offered that if he continued his cooperation, he would be exempted from Sarbazi – conscription. [According to the Iranian constitution, men older than 18 years old are required to perform military service. The length of service is 18 months-2 years].

Ali remained under tremendous stress because of the video. He had no way of finding who had sent it to him, though he was convinced it came from the Intelligence Ministry. He trusted no one anymore. He didn't want to see me. Then, after three weeks of no communication, I

received an SMS from him saying this was the end of line. I went to him. The video, he said, had clearly been taken by the ministry, who wished to threaten him in order to coerce him to do their will. Their expectations increased day by day. He didn't want to be involved with cyber crimes on the international level. But he had little choice. His father was suffering from heart disease. Ali knew that if he took his own life, it would mean disaster for his family. If the video were to be published, this would also be a disaster for his family. They didn't leave any option for him.

This is the situation facing many hackers recruited by coercion by the Iranian authorities. Days and nights, on anti-stress medication and worrying about their tomorrow. Continuous threats from the IRGC or the Intelligence Ministry. Ignored by their friends, receiving blackmail threats. And wanted by international law enforcement because of their activities.

Details of Iran's Cyber Campaign

"Today, we are in an atmosphere of a full-blown intelligence war with the US, and the front of enemies of the Revolution and the Islamic system," IRGC Commander Hussein Salami said recently, adding that, "This atmosphere is a combination of psychological warfare and cyber operations, military provocations, public diplomacy and intimidation tactics."

Cyber war in Iran is part of the military strategy of Iran's soft war. 'Iranian Cyber Army' is a name used for the regime's cyber activities on the internet.

Iran has been condemned for cyber attacks against the United States, Israel and the Arab Gulf states. But the regime has issued a blanket denial concerning all such activities.

Iran's 'Cyber Army' is a subset of the IRGC's cyber surveillance team, with a budget of $76 million and over a billion dollar investment in infrastructure . Defense Tech estimated the number of 'troops' in this army at about 2,400, with 1,200 reserves.

The plan to form Iran's Cyber Army was proposed by the IRGC in 2005. The Cyber Army manpower unit teams, after identifying professional hackers, contact them and threaten to send them to prison if they do not cooperate.

A statement from Iran's Cyber Police (FATA) said "White hat hackers are valuable people who benefit from the knowledge of cyberspace. Police identify white hat hackers, The police is in contact with these hackers, and many of these hackers express a desire to cooperate with the police. We use this nucleus to advance our goals."

Structure and targets

Iran's cyber army is divided into five sections

The first section's mission is defense. It tracks the identity of attacking hackers and thwarts their activities.

The second section 's mission is offensive, targeting infrastructure facilities belonging to countries in "opposition to the Islamic Republic", including energy, water, train networks and airports. The group also seeks to target some countries' nuclear facilities, banks and global markets.

> The Basij Cyber Council is a main center which trains volunteer hackers under the supervision of IRGC. These volunteers are called 'cyber war commandos.'

The third section is responsible for decrypting passwords and data transfer tools.

The fourth section's mission is to jam the frequencies of certain Arab and Western television channels. This group was established some months ago, and so far it has been able to jam some Persian and Arabic-language television channels.

The fifth groups mission is to carry out DDOS and DOS (denial of service) attacks against important sites in enemy countries.

The Basij Cyber Council is a main center which trains volunteer hackers under the supervision of IRGC. These volunteers are called "cyber war commandos."

Malek Ashtar Base and Kheibar Security Base are the hacking centers that have a key role in educating young talent and recruiting new staff [both Iranians and non-Iranians].

Ashianeh Group is the oldest, most active and most famous cyber security group in Iran. ´Ashianeh members are among the most active members of Iran's cyber army. Their activities have been extensively covered by IRGC affiliated news agencies under the title of "Iran's Victories". The group was established eight years ago with the aim of educating users and network administrators and improving the security level of computer networks in Iran. But in the course of its evolution, it did not adhere to these goals alone. At the present time, their activities have more of a political flavor than an educational one.

Ashianeh has carried out several projects to infiltrate foreign sites and networks. On December 21st, 2020, Tasnim, an IRGC affiliated news website, wrote " Iranian hackers managed to enter the servers of the Israeli Air Force. Israel's Cyber Structure Kneels before our hackers. Are Iron Dome Radars Hacked?"

"US federal authorities have prosecuted a zealous young Iranian hacker for allegedly being involved in a cyber attack on a number of US websites following the brutal assassination of Haj Qassem Soleimani, commander of the IRGC's Quds Force."

Operations against major US facilities, including cyber-attacks on several dams, several major US banks and power plants, and a number of cyber attacks on Saudi banks and statistical centers, a 12-hour power outage in Turkey, attacks on various Israeli centers and satellites, were all carried out via the Kheibar base.

Kheibar was established with the aim of concentrating the technical forces of offensive and cyber defense in 2012 with a combination of cyber technical forces of the technical department of the Ministry of Intelligence, the cyber department of the IRGC, and the technical forces of the Ministry of Defense and Armed Forces Support.

In 2016, the commander of Iran's cyber army, formerly stationed at the Kheibar base, Mohammad Hossein Tajik, was executed by the Iranian intelligence service. Tehran's coroner declared the cause of death to be cardiac arrest.

Tajik, born in 1981, was one of the elite students of Iran in the field of physics. He was killed in the presence of his father and a Ministry of Intelligence employee at his home in east Tehran. He had been arrested in 2014 on charges of espionage. Following the intervention of his father, he was temporarily released after six months.

Tajik's father, a member of the Quds Force and a longtime friend of Qassem Soleimani, worked with various Quds Force-affiliated organizations in the Middle East and various intelligence services on his missions from 1998 to 2013.

Another base, Malek Ashtar, is mainly focused on the field of attacking Farsi news websites and hacking the social media accounts of activists and oppositionists inside and outside the country. They established a number of branches under different names all over Iran.

> While government hackers are carrying out acts of sabotage against activists and popular anti-regime users on social media, anonymous independent groups of hackers support the opposition, especially during the recent protests, by hacking the accounts of cyber army members/IRGC propagandists, and revealing their real identities.

Counter activities by opposition cyber activists

While government hackers are carrying out acts of sabotage against activists and ´popular anti-regime users on social media, anonymous independent groups of hackers support the opposition, especially during the recent protests, by hacking the accounts of cyber army members/IRGC propagandists, and revealing their real identities.

In January 2019, One of these hack groups “Tapandegan” which is famous for targeting IRGC assets, took over the computer systems at one of the largest airports in Iran.

On the billboards and television screens at Mashhad airport, passengers saw a symbolic image of the December 2017 protests with the Popular hashtag in farsi "#national_protests" اعتراضات_سراسری

This was accompanied by the following message: “Attention, attention. We are Tapandegan. We have taken control of the computer system at Mashhad Airport as an act of protest. It has been five months since unrest has gripped the country. However, the IRGC continues to waste money, lives, and resources in Syria, Gaza, and Lebanon. We will continue our protests until they cannot silence our voices any longer. We are acting in solidarity with the courageous people of Kazerun [in the southern province of Fars, site of a violent protest on May 16]. We have just started our campaign. If you support our cause, then we ask that you share with us any crucial information including footage of protests around the country.”