GlobalResearch
Center for Research on Globalization

Israel and Iran Face Each Other in Cyberspace

By Lucas Leiroz de Almeida
Global Research, May 20, 2020
Region: Middle East & North Africa
Theme: Intelligence

Cyber warfare is one of the main bellicose activities of contemporary times. Through technologically advanced and powerful weapons, the great world powers face each other on the international stage in an invisible field, far from media attention, where the most complex networks of information and state secrets circulate. The fundamental nature of the cyber field for modern warfare is currently undeniable. More and more cases of virtual clashes between world powers are confirmed, with secret cyber warfare units being revealed day after day. Now, this confrontation seems to have definitely come to rivalry between Iranians and Israelis in the Middle East.

On May 9, a major cyberattack was registered against Iran. The main victim of the operation was the network in the port area of Bandar Abbás, in the south of the country. An unidentified source, who claims to be "an official of a foreign government", said in an interview that the attack was "very accurate", causing "total disorder" in Iranian authorities, with almost irreparable damage. He further claims that the damage was much greater than was officially reported by the Iranian government. It is possible that much information of precious strategic value was captured with this virtual attack.

Now, a recent article in The Washington Post, bringing together information from several sources – many of which are classified – states categorically that the attack was led by Israel, which reportedly carried out the operation as part of a cyberwarfare scheme.

> "The attack, which snarled traffic around the port for days, was carried out by Israeli operatives, presumably in retaliation for an earlier attempt to penetrate computers that operate rural water distribution systems in Israel, according to intelligence and cybersecurity officials familiar with the matter", writes the newspaper.

Israel recently formally accused Iran of being behind a series of "daily cyberattacks" against Tel Aviv. In his speech, Israeli Prime Minister Benjamin Netanyahu said that such attacks occur on a daily basis and are constantly monitored and repelled by Israeli security forces. Tehran not only denies involvement in the case but claims to have no participation in cyber wars. The May 9 attack was supposed to have been a retaliation for these attacks against Israel.

The director of the Iranian Maritime and Port Organization, Mohammad Rastad, confirmed on May 10 that a recent cyberattack could "damage several private operating systems in ports". Some foreign intelligence sources cited by The Washington Post on May 8 pointed out that Iran was linked to the April 24 cyberattack against at least two rural water distribution networks in Israel – part of the attacks mentioned in the previous paragraph.

In September last year, Iran's foreign minister, Mohamad Yavad Zarif, said Iran is facing a cyberwar. The minister mentioned the so-called Operation Olympic Games, which the United States and Israel reportedly launched in 2006 against the Iranian nuclear program, and the acts of sabotage carried out with the cyber weapon "Stuxnet worm". Identified in 2010, this virus is malicious code that attacks Windows operating system computers through various vulnerabilities. It was used in 2009 and 2010 to infect computers at various Iranian entities, including the Iranian nuclear plant at Bushehr, and has been detected in other countries such as Indonesia, India, Azerbaijan, Pakistan and the USA, and is apparently a cyberweapon in common use by various armed forces and intelligence agencies worldwide.

The most interesting and important of all this is not to identify who actually committed such attacks, but to recognize the problem of cyber wars in contemporary geopolitics. The current world cannot be understood by the simple duel of "visible" forces, as it was in the Cold War, where the nuclear race marked the struggle for power between nations. Today, most weapons are outside this scope of easy identification and great damage can be done to entire nations through absolutely invisible and immaterial attacks. This new reality raises the complexity of the debate about everything we know about international relations, geopolitics and international law to a new level and brings deep reflections on the world in which we live.

Apparently, the confrontation between Iranians and Israelis has reached a new stage, in which nations also face each other in cyber reality. And this will be a stage to which all armed confrontations and geopolitical rivalries on the planet will be elevated until there is a definitive international consensus on the nature of cyberspace. Perhaps, more than ever, it is necessary to think about the possibility of creating a "cyber nomos", a legal status for cyberspace in international law, where specific limits on war, crimes, espionage and terrorism in cyberspace are established. Only then, cyberattacks can be combated with formal sanctions and condemnations, without rebuttal and without the perpetuation of the conflicts.

*

Note to readers: please click the share buttons above or below. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

This article was originally published on InfoBrics.

Lucas Leiroz is a research fellow in international law at the Federal University of Rio de Janeiro.