

## Cyber Wars in Iran

The Journal of Turkish Weekly, July 24, 2010

<http://www.turkishweekly.net/news/105083/cyber-wars-in-iran-.html>

The internet is often seen as the domain of dissidents and free spirits. But the Iranian regime like many others has long recognised the importance of winning the virtual propaganda war, and the talk for the last couple of years has been of an “Iranian Cyber Army”, a band of dedicated regime loyalists who attack opposition websites and other virtual targets.

But untangling myth from reality in this murky world is difficult. Has the Iranian Revolutionary Guards Corps, IRGC, really deployed one of the largest forces of hackers on the planet, or is it smoke and mirrors, designed to intimidate dissident web users?

The years 1999 to 2009 were a golden decade for freelance hackers in Iran, “an era of chaos”, as a network security expert in the country describes it. With no comprehensive internet legislation or other barriers, groups of young hackers operated at will, even attacking sensitive government websites belonging to the army, the prosecutor general and even the space agency.

A member of “Emperor”, one of these groups, says it was once commissioned by a local firm to destroy a government database, while in the 2005 presidential election, it was asked to hack into two candidates’ websites.

Another group, known as “Iran Hackers Sabotage”, consisted of two 21-year-old software engineering students and one 18-year-old mathematics student who rose to fame for defacing the Guantanamo prison website.

Hackers continue to be active – a few weeks ago, Iranian police announced they had identified four hackers responsible for the cyber-theft of five million dollars from banks in Iran.

But the best-known groups have since faded away, replaced in the public imagination by hackers of a different breed.

The term “Iranian Cyber Army” first emerged when a number of opposition websites abroad as well as Twitter and Baidu were hacked last year. Although the attack resulted in no more than a brief disruption of activity, the name and reputation were made – though what they refer to precisely remains unclear.

No government agency has acknowledged control of the cyber army, but it is commonly believed that the Revolutionary Guards are behind it.

According to an IT specialist at Imam Hussein University in Tehran, “Between 2005 and 2007, the IRGC’s political bureau and strategic research centre took the concept of bringing confrontation with the United States and Israel into cyberspace and transformed it from an idea into a costly operational programme, designed to take on domestic websites run by the opposition and also to penetrate foreign websites.”

In May 2010, Ebrahim Jabbari, a provincial Revolutionary Guards commander, went as far as to claim that the IRGC had the world's second-largest cyber army at its disposal.

A 2008 report on the US website defencetech.org suggested that the IRGC's cyber warfare capacity placed it in the world's top five. The report was a "threat assessment" from a US perspective, but when it was translated eight months later, the Iranian authorities took it as a compliment and turned it to their advantage for propaganda purposes.

The network security expert, who used to work for the IRGC himself, says many of the old freelancers have been coopted into the new "army", in some cases in return for having past sins overlooked.

While its links to aggressive hacking are unconfirmed, the IRGC does have a publicly-acknowledged defensive arm.

Set up in 2007, its existence was first publicised the following year in a news item on the arrest of managers of online porn sites.

In the wake of last year's election, it showed it had political aims as well, announcing the detention of members of two internet networks. One of them, Iranproxy, had distributed 86 million sets of free software allowing users to create "virtual private network" and use proxy sites to get round web blocking. Tother was run by civil rights activists who disseminated information about political arrests and detentions.

In addition to paid cyber warriors and web monitors, the Iran regime also has an ally in the shape of the private IT firm Ashiyane Security Group, which regularly makes the headlines with coordinated cyber-attacks.

During the Israel incursion into Gaza last year, Ashiyane took down 500 websites in the country, including those belonging to Mossad and the then defence minister Ehud Barak. Last December, it claimed to have hacked into 700 Israeli websites including the postal services.

At about the same time, Ashiyane also attacked the website of NASA, the US space agency, which it said had shown a lack of respect for the late Ayatollah Ruhollah Khomeini. It uploaded a picture of Khomeini to the NASA site, with the inscription, "Our war is an ideological war and knows no borders or geography. As long as there is blasphemy and apostasy, there will be battle, and where there is battle, so are we."

When Sunni Arab hackers brought down the Ahl al-Bayt site a server that hosts most Shia religious websites in Iran, including those of leading ayatollahs, Ashiyane also responded in kind, attacking five servers and defacing 300 websites in the Arab world.

The talk on the web is that Ashiyane is closely linked to the IRGC, but no documentary evidence proving or disproving this has yet come to light. The group's head, Behrouz Kamaliyan, has also indicated that it is not linked to the purported cyber army.

Kamaliyan, 28, started hacking at the age of 16. Like many of his peers, he hacked into government websites, but in his case it was to persuade them they needed his help to improve web security. He later went on to set Ashiyane up as a legitimate business, officially specialising in net security and unofficially, in undermining Iran's enemies on the web.

Last year, his company designed and produced a firewall system called Apadana, intended to protect web-based information from hackers. He told the Fars news agency that the system will allay any concerns that confidential data could be lifted from Iranian security, intelligence and defence websites if they use firewall systems designed abroad.

Like President Ahmadinejad, Kamaliyan is deeply hostile to Israel. He has vowed to undermine that country's e-government system, and believes that the Israeli state has no right to exist and should therefore be denied a virtual existence, in the shape of its country domain name.

Some analysts argue that the might of the Iranian regime's cyber-allies is overstated.

While Ashiyane boasts of attacking hundreds of websites at a time, other experts say it does so without much effort, by penetrating a single server where the sites are hosted.

Analysts interviewed for this report said exaggerated reporting in the state-run media had succeeded in persuading Iranians that the IRGC was a power to be reckoned with in cyberspace. Yet the extraordinary feats claimed by these cyber-warriors were technically simple and could have been done by a teenager with no specialist training.

A journalist whose own blog fell victim to state filtering, believes there is an element of PR in all the official talk about cyber-warfare, adding that he thinks the main aim is to cow dissidents who use the web to express their views.

As for the regime's ability to protect its own sites from attack, the network security expert said, "The truth is that the majority of servers and government websites in Iran are as full of holes as Swiss cheese, and until these holes are filled, it is better not to annoy the mice."