# Group Planning to Hack Bank in Iran Arrested

**OE Watch Commentary:** The Islamic Revolutionary Guard Corps' (IRGC) Passive Defense Organization usually defines cyber defense as efforts to prevent foreign infiltration of Iranian government and national security systems, and press releases from Iran's Cyber Police often focus on either morals crimes or stopping those using the internet to ridicule or insult the Islamic Republic's religious leadership. The accompanying excerpted article, however, reveals another element of cybercrime in Iran: insiders compromising systems for profit. The episode also sheds light on the nature of the Iranian security state. It references in passing the Intelligence Ministry's maintenance of provincial offices to investigate and handle what in many other states would be a simple police matter. The Intelligence Ministry involvement in this bank hacker case also suggests that, despite the proliferation of organizations involved in cyber policy in Iran, the Intelligence Ministry remains paramount. Unclear is who the potential victim(s) would have been. Ordinary Iranians do not trust Iranian banks and often try instead convert their savings to gold or hard currency, like US dollars or Euros. This raises the possibility that the hackers sought to embezzle from a state-owned or IRGC-owned enterprise. **End OE Watch Commentary (Rubin)**

The Official Seal of Islamic Republic of Iran Cyberspace Police (FATA).
*Source: By MrInfo2012 [Public domain], from Wikimedia Commons, https://commons.wikimedia.org/wiki/File:IRI.NAJA.FATA_(New).svg.*

*"A group of hackers... sought to infiltrate, sabotage, and embezzle."*

Source: "Dastgiri Yek Gorueh Hakari keh Ghasad-e Ekhlal far Nezam-e Banki Dashtand (Arrest of a Group of Hackers Aiming to Disrupt the Banking System)," *Fars News Agency,* 28 May 2018. www.farsnews.com/13970307000323

*Hasan Rafiqi said: According to reports from the Intelligence Ministry's office for the Esfahan province, a group of hackers with the cooperation of two employees from one of the provincial banks, sought to infiltrate, sabotage, and embezzle from customer accounts. But, after a judicial order, and the members of this group were arrested before they could commit any crimes. The Esfahan prosecutor said those arrested had confessed that they intended to infiltrate the banking system and access customer information in order to conduct criminal acts. According to the Esfahan prosecutor, nine people were arrested in this regard.*

# Cyberspace Should Promote Religious Teaching

**OE Watch Commentary:** The Islamic Republic of Iran is, at its heart, an ideological state dedicated to the promotion not simply of Shi'ism, but of Islam more broadly. While much of the debate surrounding Iran's cyber policy focuses on its potential offense against outside powers or attempts to constrain free access to the internet and social media, the accompanying excerpted article highlighting a speech by the Minister of Culture and Islamic Guidance underlines the Islamic Republic's efforts to use new technology to export its religious vision. While putting Quranic commentaries and other religious texts online might on one hand in theory add an important resource to those engaged in the study of Shi'ism, on the other it may signal greater aggressiveness in Iranian efforts to fulfill its constitutional imperative to export revolution. After all, Morocco has now twice broken diplomatic relations with Iran in part because of Iranian efforts to proselytize Shi'ism among its population. Often, this proselytization occurs online as a mechanism to avoid ordinary security. Indeed, online proselytization can be an effective tool. Both Al Qaeda and ISIS attracted an international array of recruits and encouraged lone wolf attacks based on magazines and texts placed online. Shi'ism, of course, does not necessarily equate with extremism—indeed, theological and historically, it is anything but extreme—but if the Iranian government decides to increase its online presence under the guide of religious education, it efforts would likely tend toward promotion of extremism. **End OE Watch Commentary (Rubin)**


Abbas Salehi.
*Source: Islamic Republic News Agency, http://img8.irna.ir/1397/13970324/82942803/n82942803-72388065.jpg.*

*"The use of cyberspace for dissemination of the Quran should be maximized."*

Source: "Quran dar Fezayi Mojazi ra Jedi Begerim (We Must Take Seriously the Quran in Cyberspace)," *Islamic Consultative Assembly News Agency*, 14 June 2018. https://goo.gl/1y76uh

*The minister of culture and Islamic guidance, with emphasis on getting the Quran into cyberspace, said, the Quran must emerge and appear in this space, and the use of cyberspace for the publication of Quranic texts and commentaries should be maximized. Sayyid Abbas Salehi pointed out the importance of new communication technologies and social networks on one hand and, on the other, the importance of the Quran in cyberspace, and remarked, "This space has become a reality in our lives today and therefore, Quranic topics and issues should be seen more deeply in the digital space…."*

*A member of the Supreme Council of the Cultural Revolution, [Salehi] said: "We believe that the use and enjoyment of digital and virtual space will be a positive step towards utilizing the potential of this area in promoting the dissemination of Quranic and religious teachings.*