AMERICAN FOREIGN POLICY COUNCIL

Iran Democracy Monitor No. 219

August 6, 2021 **Ilan I. Berman**, **Cody Retherford**, **Maya Walborsky**

Related Categories: Cybersecurity and Cyberwarfare; Democracy and Governance; Human Rights and Humanitarian Issues; Resource Security; Middle East; Iraq; Iran

IRANIAN HACKERS HARD AT WORK
Hacker groups with ties to Iran's Islamic Revolutionary Guard Corps (IRGC) are known to have recently targeted a range of American military personnel and U.S. Middle East scholars. In one initiative, a group called "Tortoiseshell" used online fake personas to connect with targets in the U.S. military and defense contractors. The hackers posed as recruiters to drive targets to various sites - such as fake domains that spoofed legitimate job search sites - where they were tricked into clicking malicious links that would infect their devices with spyware. The investigation found that the malicious software used by the hackers was developed by Mahak Rayan Afraz, an IT company based in Tehran with ties to the IRGC.

At the same time, another IRGC-connected hacker group targeted Middle East scholars and journalists through credential harvesting. According to the security firm Proofpoint, an Iranian threat group that has been designated as TA453 has been conducting spear-phishing attacks in an attempt to steal sensitive material such as information on foreign policy, dissident movements and U.S.-Iran nuclear negotiations. (*GovInfoSecurity*, July 14, 2021; Reuters, July 15, 2021)

WATER PROTESTS... AND THE REGIME RESPONSE
Over the past few weeks, thousands of Iranians have taken to the streets in cities and towns throughout the Islamic Republic to protest the country's deepening hydrological crisis. Beginning in mid-July in the oil-rich province of Khuzestan, protests broke out over water shortages brought about by deepening drought conditions and longstanding governmental mismanagement. Since then, the unrest has spread throughout the country, including to the capital city of Tehran.

The Iranian regime has responded predictably. Hundreds of protestors have been arrested to date, and dozens have been killed in clashes with government forces. The Iranian regime also moved quickly to disrupt telecommunications and the internet, relying on lessons learned from successfully suppressing earlier rounds of domestic protests over the past several years. (*CNN*, July 25, 2021; *Radio Free Europe/Radio Liberty*, July 27, 2021)

[EDITORS' NOTE: The latest protests are of enormous potential significance. The hydrological situation in Iran has steadily worsened in recent years. A 2019 study by the World Resources Institute, a U.S. NGO, identified Iran as one of the most "water-stressed" nations in the world. (See *Iran Democracy Monitor* no. 199.) This crisis has been greatly exacerbated by decades of governmental mismanagement, which has created resource scarcity that now affects every strata of Iranian society - thereby providing a unified basis for opposition to the regime.]

TEHRAN TURNS UP THE HEAT IN IRAQ
As the United States increasingly contemplates a smaller footprint in Iraq, Iranian proxy groups in the country and beyond are stepping up their activities. Last month, IRGC intelligence chief Hossein Taeb reportedly met with Shi'ite militias in the country and urged them to step up their attacks on U.S. forces as American forces draw down. The Biden administration is now reportedly mulling a fundamental shift in the U.S. presence there to a purely advisory role. That change could come as early as the end of the current year, and Iranian officials appear to be interested in stepping up the pressure on Washington as a way of accelerating this timeline. (Reuters, July 13, 2021; *Politico*, July 22, 2021)