BESA PERSPECTIVES
THE BEGIN-SADAT CENTER FOR STRATEGIC STUDIES

The Ever-Growing Iranian Cyber Threat

by Mansour Piroti

BESA Center Perspectives Paper No. 2,160, September 26, 2021

EXECUTIVE SUMMARY: The Iranian regime has been a considerable threat to global cybersecurity ever since 2012, when it committed cyberattacks on US financial institutions in retaliation for the high-profile Stuxnet attack on its nuclear program. In the wake of the Stuxnet attack, the Tehran regime vastly ramped up its cyber capabilities, transforming itself from a third-tier cyber power into one that poses a serious threat.

The cyber transformation of Iran was initiated by a decree issued in 2012 by Supreme Leader Ali Khamenei that established the Supreme Council of Cyberspace, which was tasked with creating a strategy and a blueprint for information control at home and intelligence gathering abroad. To achieve these goals, the Council established a sophisticated and multi-layered cyber operations bureaucracy. Within three years, Iran's budget for cyber development had increased by 1,200%.

In the decade since the establishment of the Council, Iran is believed to have been responsible for a wide range of cyber operations around the world. Industry pillars of the region's economy, academics, and defense companies have been targeted in these attacks. Aramco and RasGas, the Saudi and Qatari petroleum companies, have both been frequent victims. In 2013, Iranian hackers penetrated the flood control system of the Bowman Avenue Dam in Rye Brook, New York, and the same group of hackers was implicated in separate attacks on three US financial firms. In 2014, regime-linked proxies hit the Sands Casino in Las Vegas with destructive malware.

These attacks were designed to gather detailed information, not affect operations. The information was meant to be used against the victims should diplomatic relations change.

In 2016, a destructive virus called Shamoon hit several Saudi oil organizations and ministries. Shamoon, a reverse-engineered version of Stuxnet, destroyed hard drives, wiped data, and prevented computers from turning on. In 2017, a version of this virus targeted the Italian oil company Saipem, taking down hundreds of company servers and personal computers in the UAE, Saudi Arabia, Scotland, and India. A similar attack was conducted against Bahrain's national oil company, Bapco, in 2019. This form of aggression reflects a shift in the regime's cyberterrorism strategy away from information-gathering and toward sophisticated attacks that cause immediate damage.

Iran also maintains a cyberattack capability for the purpose of countering domestic dissent. After the 2009 election protests in Iran, the regime shut down the internet repeatedly to control information and hijack public opinion. In November 2019, Iranian security forces killed hundreds of unarmed protesters and bystanders during five days of protests following the government's overnight announcement of a significant increase in the price of fuel. This deadly crackdown was accompanied by a withdrawal of internet access for most of the population. In February 2021, internet bandwidth was throttled following days of bloody protests across the Balochistan province over the killing of Baloch fuel traders.

The regime considers a domestic uprising to be an existential threat. As Iranian protest organizers expand their base on the internet, the regime revokes digital rights and internet freedoms inside the country. It infiltrates the websites and email accounts of political dissidents and routinely censors online content and communications. The regime also employs disinformation campaigns in which it uses forged social media accounts to broadcast fake stories to influence public opinion and stoke social tensions.

Empowered by recent political changes, the IRGC is lobbying for parliamentary action to update the laws governing the internet in Iran. Its goal is to develop a national intranet and disconnect Iran from the global internet. Along the lines of this effort, regime-sponsored front companies have produced spyware-enabled mobile apps and VPNs for cyber-surveillance and repression. Some are available on global mobile app marketplaces like Google Play, the Apple Store, and GitHub, potentially exposing millions of citizens in Iran and around the world. These apps enable the regime to censor content, spy on individuals, and even make money.

The Islamic regime's cyber operations not only surveil internal opposition groups and political opponents but also target the Iranian diaspora, using spear-phishing and SMS messages to persuade targets to open malicious links or attachments. In February 2021, the Dutch public broadcaster reported that

the regime had used a server in the Netherlands linked to a base in Iran to gather intelligence on Iranian dissidents.

Mansour Piroti is a freelance writer based in Iraqi Kurdistan.