AMERICAN FOREIGN POLICY COUNCIL

The Other Iranian Threat

April 16, 2018 **Ilan I. Berman** *Alhurra*

Related Categories: Cybersecurity and Cyberwarfare; Democracy and Governance; Islamic Extremism; Terrorism; Iran; Middle East

Whatever happened to the Iranian cyberthreat? Not all that long ago, American officials were preoccupied with the growing disruptive capabilities that the Islamic Republic had begun to demonstrate on the World-Wide Web. That, however, was before the start of negotiations over Iran's atomic program in 2013. Those talks allowed Iran's cyber activities to recede from public view, as policymakers in Washington focused their attention on nuclear diplomacy with Tehran, while Iranian hackers temporarily became more cautious in their choice of targets and the visibility of their attacks. More recently, worries about Iran's cyber capabilities have taken a back seat to concerns regarding Iran's growing conventional military might, and its mounting regional adventurism in places like Syria and Yemen.

But now, Iran's movements in cyberspace are receiving some much-needed renewed attention, thanks to a new report from one of the world's leading cybersecurity firms, which warns the cyberthreat posed by Iran is growing in both sophistication and menace.

"Throughout 2017, [we] observed a significant increase in the number of cyber attacks originating from threat actors sponsored by Iran," notes the Mandiant corporation in its latest study of global cyber threats. "While they have captured notoriety over the past year, especially for their destructive attacks, much of their espionage activity has gone unnoticed. Their list of victims currently spans nearly every industry sector and extends well beyond regional conflicts in the Middle East."

The report continues: "For some time, these threat actors were primarily a nuisance consisting of a loose collective of patriotic hackers who conducted web defacements, distributed denial of service (DDoS) campaigns and occasional destructive malware attacks." But over the past eight years, since the 2010 malware attack on Iran's nuclear infrastructure popularly known as Stuxnet, the Islamic Republic "has increased its cyber espionage capabilities and is now operating at a pace and scale consistent with other nation- state sponsored [cyber threat] groups."

The results have been notable. "Iranian threat actors have compromised a variety of organizations, but recently they have expanded their efforts in a way that previously seemed beyond their grasp. Today they leverage strategic web compromises (SWC) to ensnare more victims, and to concurrently maintain persistence across multiple organizations for months and sometimes years. Rather than relying on publicly available malware and utilities, they develop and deploy custom malware. When they are not carrying out destructive attacks against their targets, they are conducting espionage and stealing data like professionals."

These activities have dramatically expanded the cyber threat posed by Iran. According to Mandiant's experts, Iran is can now be seen as "the new China" in cyberspace – a persistent and prolific threat actor that is rapidly increasing in both technical sophistication and ambition. Indeed, of the four new threat groups christened by Mandiant as "advanced persistent threats" in cyberspace over the past year, all but one originated in Iran.

What does this mean for America and its international partners? For years, U.S. intelligence professionals have worried over Iran's growing investments in its cyber capabilities – which have been a major focus for the country's current, "reformist" president, Hassan Rouhani. Since taking office in 2013, Rouhani has reportedly increased Iran's federal budget for cyber activities as much as twelvefold, thereby catapulting the country into the position of a "top-five world cyber power." As of yet, however, the United States and its allies lack anything resembling a coherent doctrine for deterring or responding to the resulting, increasingly sophisticated attacks and espionage activities that Iran is carrying out in cyberspace.

Mandiant's report is a timely reminder of the need to develop one. As the Trump administration edges toward withdrawal from the 2015 nuclear deal, it would do well to remember that Iran has the capacity to retaliate against renewed economic and political pressure on a number of fronts – including in cyberspace. It would do even better to start preparing for such a possibility, and so would its allies.

Ilan Berman is Senior Vice President of the American Foreign Policy Council in Washington, DC.