Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

January 13, 2020

Iranian Offensive Cyberattack Capabilities

Threat Evolution

Iran's use of cyberspace has evolved from an internal means of information control and repression to more aggressive attacks on foreign targets. The regime has been developing its own cybersecurity software and internet architecture in order to protect and insulate its networks, and it has been developing technological cyber expertise as a form of asymmetric warfare against a superior conventional U.S. military.

Iran also has a history of using cyberattacks in retaliation against the United States. In 2010, a computer worm known as Stuxnet was discovered by cybersecurity researchers to have infiltrated the computers that controlled nuclear centrifuges in Iran, causing physical damage and preventing operation. The Stuxnet worm was reported to have been a joint effort between the governments of the United States and Israel. Following the discovery of the Stuxnet malware, U.S. assets experienced an increase in the severity and duration of cyberattacks originating in Iran.

Recent events have heightened interest in Iran's current cyberattack capability with respect to U.S. vulnerabilities.

Iranian Cyber Organization

Since the advent of the Stuxnet worm, Iran has been investing resources in developing its own cyber forces and organizations. Some of these entities reside within the government and military, while others appear to operate more independently. Some focus more on defensive capabilities but may operate in concert with military units conducting offensive operations. The information below draws from unclassified sources.

Government Entities

Iran Cyber Police. A law enforcement unit, the Cyber Police is responsible for tackling what it considers internet crimes. To this end, the unit monitors online activity within Iran, including infiltrating websites and email accounts of political dissidents.

Ministry of Intelligence and Security (MOIS). Similar to the U.S. National Security Agency, MOIS is responsible for signals intelligence and collecting information from electronic communications.

Supreme Council of Cyberspace. Also known as the High Council of Cyberspace, this body coordinates cyberspace policy for the Iranian government and coordinates between offensive and defensive cyber operations.

National Cyberspace Center (NCC). An entity of the Supreme Council of Cyberspace, the NCC is largely concerned with information content and development of internal internet security controls. The NCC is also tasked with "preparing for a cultural war" between Iran and its enemies, according to the 2013 NCC Statute issued by Iran.

Islamic Revolutionary Guard Corps (IRGC). A branch of the Iranian Armed Forces, this military force oversees offensive cyber activities.

IRGC Electronic Warfare and Cyber Defence Organization. This organization provides training courses in cyber defenses and denies access to and censors online content and communications.

Basij Cyber Council. Considered a paramilitary force, Basij comprises nonprofessionals, using volunteer hackers under IRGC specialist supervision. These volunteers are sometimes referred to as "cyber war commandos."

National Passive Defense Organization (NPDO). Formed for infrastructure protection, one of the NPDO's main roles according to analysts is to use "all national cyber and non-cyber resources to deter, prevent, deny, identify, and effectively counter any cyberattack against ... Iran's national infrastructure by either hostile foreign states or [domestic] groups supported by them."

Cyber Defence Command. Also known as Cyber Headquarters in the Iranian military, this group conducts offensive cyber operations along with the Basij Cyber Council. The command may have been created as a corollary to the U.S. Cyber Command.

Proxies

Iran has been known to employ proxies to conduct cyber operations. These range from either patriotic or financially motivated individual hackers, to private sector contractors and quasi-governmental organizations. Given the amount of control that the Iranian regime exercises over the internet activity of its citizenry, one may assume that while the actions of individuals may not be state-directed, it is almost certainly state tolerated or even encouraged. The use of proxies also allows the regime to maintain plausible deniability for the attacks, thereby avoiding escalation. However, readily identifiable signatures in the computer code suggest that the Iranian government endeavors to take the credit for attacks on foreign entities as a demonstration of ability.

Mabna Institute. A group of private sector contractors that conduct computer intrusion, wire fraud, and data theft at the behest of the government of the Islamic Republic of Iran and the IRGC.

Iranian Cyber Army. IT specialists and professional hackers. The Cyber Army has not been directly linked to the IRGC, but Iranian government officials refer to using it to hack "enemy sites," diverting internet traffic, and hacking into foreign media sites and social media platforms.

Cyberattack Methods

Since at least 2012, Iranian cyberattacks have been advancing from simple website defacements to denial of service and other disruptive or destructive forms of attack. These include distributed denial of service (DDOS) attacks that prevent access to target websites and more destructive attacks that destroy data or disable computers entirely.

Website Defacement. Cyberattacks that manipulate data and images on a website or redirect traffic to a new web page.

Data Breach and Theft. Intrusions into computer systems that allow extraction of large amounts of otherwise protected data.

Denial of Service. Cyberattacks that flood a computer or network with traffic, rendering it inaccessible to users.

Destructive Attacks. Cyberattacks that destroy applications and computers within a target network with damage that could possibly equal that of a kinetic attack. An example is a "wiper" attack, where an infected computer hard drive is overwritten or cleared of data.

Iran-Attributed Incidents

Saudi Aramco. In 2012, wiper malware known as Shamoon damaged computers and delayed oil production after targeting Saudi Aramco and other energy companies in the Middle East. U.S. government officials linked the attack to Iran.

Sands Casino, Las Vegas. In 2014, destructive attacks accessed and destroyed data on the network of the Sands Hotel and Casino, owned by a political donor seen as pro-Israel and anti-Iran. The U.S. Director of National Intelligence attributed this attack to the Iranian government in a Statement for the Record to the House Permanent Select Committee on Intelligence.

U.S. Banks. From 2011 to 2013, DDOS attacks in which banks' websites, including Bank of America and Wells Fargo, were overwhelmed with internet traffic, preventing customer access for a period of time. In March 2016, the U.S. Department of Justice indicted seven Iranian actors contracted by the IRGC who were said to have cost the banks millions of dollars in remediation.

Twitter and Facebook. In 2009, Twitter web traffic was redirected to a page for a group claiming to be the Iranian Cyber Army. In 2018, Twitter announced that it had removed 2,617 Iranian accounts that were engaging in "malicious activity." In May 2019, Facebook stated that it had removed Iranian-linked Facebook accounts, pages, and groups as well as Instagram accounts. While much of this activity involved trolling and other influence operations, social media platforms could also be used to coordinate cyberattacks.

Rye, New York Dam. In 2013, an Iranian employed by a company contracted by the IRGC was able to access remotely the supervisory control and data acquisition (SCADA) systems of the Bowman Dam in Rye, NY. This gave access to information regarding the status and operation of the dam, possibly compromising its functioning. The Iranian was indicted by the U.S. Department of Justice in 2016.

Cyber Data Theft Ring. From approximately 2013 to 2017, cyber thieves associated with the Mabna Institute targeted intellectual property and other data from 144 U.S. universities, the U.S. Department of Labor, the Federal Energy Regulatory Commission, the state of Hawaii, and the state of Indiana, as well as companies and organizations outside the United States. The Department of Justice indicted nine Iranians for these incidents in 2018.

While there are many reports of Iran's increasingly sophisticated cyberattack capability, previous incidents also can be attributed to poor security controls of the targets. However, discovery of sophisticated malware such as Stuxnet could allow for reverse engineering, giving Iran its own destructive capability.

Possible Iranian Cyber Response to Recent U.S. Action

On June 22, 2019, Christopher C. Krebs, Director of the Department of Homeland Security's (DHS's) Cybersecurity and Infrastructure Security Agency (CISA), issued a statement that "CISA is aware of a recent rise in malicious cyber activity directed at United States industries and government agencies by Iranian regime actors and proxies…. Iranian regime actors and proxies are increasingly using destructive 'wiper' attacks, looking to do much more than just steal data and money." On January 2, 2020, the day IRGC major general Qasem Soleimani was killed in a U.S. air strike at Baghdad International Airport, Krebs linked back to this statement on his social media account.

On January 4, the DHS National Terrorism Advisory System issued a bulletin warning that "Iran maintains a robust cyber program and can execute cyberattacks against the United States. Iran is capable, at a minimum, of carrying out attacks with temporary disruptive effects against critical infrastructure in the United States." The bulletin warned of the potential for cyber retaliation in response to the U.S. military strike in Baghdad. Also on this day, hackers claiming to represent the Islamic Republic of Iran hacked and defaced several U.S. websites. CISA representatives did not confirm that this attack was sponsored by the Iranian government.

In the days following the death of Soleimani, the U.S. Selective Service System website was disabled due to high volumes of web traffic. Random U.S. citizens had been receiving text messages that indicated a draft had been reinstated for an imminent war in Iran. The origin of these text messages is unknown.

Catherine A. Theohary, Specialist in National Security Policy, Cyber and Information Operations

IF11406

Disclaimer