PART 3:
MAJOR IRANIAN CYBERATTACKS AROUND THE WORLD

The following section presents the major attacks that Iran has conducted to date against states around the world, while attacks against Israel are presented in the next section.[48]

Disruptive and destructive (CNA) attacks: Some of the earliest attacks attributed to Iran were carried out by the Iranian Cyber Army, a collection of IRGC-affiliated hackers. In 2009, in response to the mass demonstrations that erupted following the presidential elections held that year, the Iranian Cyber Army launched a number of web defacement and DDoS (distributed denial of service) attacks against websites and news outlets affiliated with opposition groups.[49]

In 2012–2013, apparently in response to the Stuxnet operation, an Iranian hacking group launched DDoS attacks against 46 major American financial institutions, including J.P. Morgan, Chase, Wells Fargo, and American Express. Known as the "Abadil" attacks, they were launched on 176 different days and locked customers out of their accounts. The immediate cost was mostly reputational: diminished customer faith in the ability of these institutions specifically and of the American banking system generally to provide secure financial services. The long-term cost to the American financial industry, however, was immense, as these and other financial institutions were forced to spend billions of dollars on highly sophisticated cyber defenses.[50]

In 2012 Iran launched one of the most destructive cyberattacks ever, against Saudi Arabia's national oil company, Aramco. The "Shamoon" attack

48 In a few of the attacks presented in this section, Israel was also a target, but a secondary one.

49 United Against Nuclear Iran, "The Iranian Cyber Threat," (September 2022), 5–8.

50 Sanger, *The Perfect Weapon,* 50; Loudermilk, "Iran Crisis"; United Against Nuclear Iran, "The Iranian Cyber Threat," (September 2022).

erased data from 30,000 computers and 10,000 servers, nearly obliterating Aramco's corporate information structure and bringing the company to the verge of collapse. Aramco was unable to process automated transactions, employees had to process billions of dollars' worth of oil trades manually, and for a few days the company was even forced to give oil away for free. A similar attack was conducted shortly thereafter against Qatar's natural gas authority, and the Shamoon malware subsequently resurfaced on a number of occasions, erasing data from thousands of computers in Saudi Arabia's Civil Aviation Agency and other organizations in 2016; targeting 15 Saudi government agencies and organizations in 2017; and targeting energy and telecommunications firms, and government agencies in 2018.[51]

In 2013 the Iranians succeeded in gaining control over the floodgates of a dam in New York. Although the attack was subsequently found to have been of limited consequence, it generated deep concern at the time over Iran's ability to damage critical infrastructure and had considerable impact on American thinking. By 2021 US intelligence concluded that Iran had, indeed, developed the ability to conduct effective attacks against critical US infrastructure.[52]

The 2015 nuclear deal (the Joint Comprehensive Plan of Action [JCPOA]) was a focus of particular Iranian cyber activity. Prior to its signing, Iran reportedly prepared attacks against American and European electric grids, water plants, transportation systems, financial institutions, and more.[53] Another attack

51 Sanger, *The Perfect Weapon,* 51–52; Reuters, "Aramco Says Cyberattack Was Aimed at Production," *New York Times*, December 9, 2012; Sulmeyer, *Cyberspace*, 37; Denning, "Explainer"; U.S. Cyberspace Solarium Commission, *Report*, 12; Siboni, Abramski, and Sapir, "Iran's Activity in Cyberspace," 22.

52 Shimon Prokupecz, Tal Kopan, and Sonia Moghe, "Former Official: Iranians Hacked into New York Dam," *CNN*, December 22, 2015; Dustin Volz and Jim Finkle, "U.S. Indicts Iranians for Hacking Dozens of Banks, New York Dam," *Reuters*, March 24, 2016; Sanger, *The Perfect Weapon,* 47–48; Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," (2021), 14.

53 Siboni and Kronenfeld, "Iran and Cyberspace Warfare," 31; Siboni, Abramski, and Sapir, "Iran's Activity in Cyberspace," 22; Brewster, "Persian Paranoia"; Courtney Kube, Carol E.

destroyed data on the networks of a Las Vegas casino, owned by a prominent American Jewish supporter of Israel and outspoken critic of the nuclear deal. The US withdrawal from the deal in 2018 and the ensuing policy of "maximum pressure" against Iran spurred renewed attacks, including ones that erased computer data from over 200 firms dealing with infrastructure, aviation, manufacturing and engineering in the United States, United Kingdom, Germany, Saudi Arabia, India, and elsewhere.[54]

In 2019, in what may have been tests of their ability to cause widespread disruption in the future, suspected Iranian hackers attacked Bahrain's National Security Agency, Ministry of Interior, First Deputy Prime Minister's Office, Electricity and Water Authority, and Aluminum Bahrain, one of the world's biggest smelters. The attacks were reportedly similar to the Shamoon malware attack against Saudi Aramco. In 2020 Dustman malware, which also had similarities to Shamoon, was used to attack Bahrain's national oil company. In this case, only a portion of the firm's computers were temporarily disrupted.[55]

In 2021 Intelligence Group 13, a secretive Iranian cyber unit, planned an attack against critical infrastructure in a number of Western countries, although it is unclear whether it actually intended to conduct the attack at the time, or if it was collecting information for future use. Some of the attacks were designed to cause disruption, including of the automatic gauges of gas

Lee, Dan De Luce, and Ken Dilanian, "Iran Has Laid Groundwork for Extensive Cyberattacks on U.S., Say Officials," *NBC News,* July 20, 2018.

54 Anderson and Sadjadpour, *Iran's Cyber Threat,* 40; Tabatabai, *Iran's Authoritarian Playbook,* 17; McMillan, "Iranian Hackers Have Hit Hundreds of Companies"; Loudermilk, "Iran Crisis"; Nicole Perlroth, "Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies," *New York Times*, February 18, 2019; Raphael Satter, "AP Exclusive: Iran Hackers Hunt Nuclear Workers, US Targets," *AP*, December 13, 2018.

55 Bradley Hope, Warren P. Strobel, and Dustin Volz, "High-Level Cyber Intrusions Hit Bahrain Amid Tensions With Iran," *Wall Street Journal*, August 7, 2019; Catalin Cimpanu, "New Iranian Data Wiper Malware Hits Bapco, Bahrain's National Oil Company," *ZDNet*, January 8, 2020; King Faisal Center for Research and Islamic Studies, *Iran's Cyberattacks Capabilities*, Special Report (January 2020), 31.

station tanks, which could have caused them to explode; of ballast systems in cargo ships, which could have caused severe damage; and of maritime communications.[56]

In 2021 Iranian hackers attempted to damage computer systems at Boston Children's Hospital, one of the largest pediatric centers in the United States. Had the attack succeeded, it could have affected both ongoing and emergency medical care. The motives for the attack are unclear, but it may have been part of a broader ransomware campaign by hackers affiliated with Charming Kittens (a.k.a. APT34). Separately, hundreds of targets in the United States, United Kingdom, Australia, Canada and Russia were attacked, including power plants and other critical infrastructure sites. The victims appear to have been targets of opportunity, whose computer systems were found to be vulnerable to attack, rather than carefully chosen ones.[57]

Turkey's attempts to normalize relations with the United Arab Emirates, Saudi Arabia, and Israel in 2021 were the apparent motive for spear phishing attacks by Static Kittens (a.k.a. MuddyWater) against high-profile governmental and private Turkish websites. Seemingly legitimate text messages from the Turkish Ministries of Health and the Interior were used to lure targets into downloading malicious links. The attacks may have been a continuation of earlier attacks against Turkish electric firms and universities, conducted from 2015 onward.[58] A number of Iranian ransomware attacks against governmental

56 Yonah Jeremy Bob, "Secret Iran Hacking Plans Against West Revealed – Report," *Jerusalem Post*, July 27, 2021.

57 Dustin Volz, "FBI Chief Blames Iran for Cyberattack on Boston Children's Hospital," *Wall Street Journal*, June 1, 2022; David Braue, "Iranian Hackers Targeting Australian Infrastructure," *ACS*, September 26, 2022; Nassim Khadem, "Australians Urged to be Vigilant Against Continued Cyber Attacks From Iran's Regime," *Australian Broadcasting Company*, January 24, 2023.

58 Menkse Tokyay, "Iran-Linked Hacker Group Targets Turkey's Cyber Network," *Arab News*, February 17, 2022.

and commercial targets in India, including defense, education, and banking systems, took place in 2022.[59]

In 2022 Iran lashed out at Albania, in what may have been the most destructive cyberattacks against a NATO ally since a Russian attack against Estonia 15 years earlier. Albania had become the subject of Iranian ire in 2014, when it agreed, at the request of the United States, to give asylum to the Mujahedin-e Khalq.[60] The hackers, probably Charming Kittens, had already penetrated Albanian government servers a year earlier but now launched a series of wiper attacks that crippled computer systems and deleted information belonging to Albania's intelligence service, police, and border guards. The identities of over 1,000 undercover police informants were also leaked on Telegram, along with the personal banking data of over 30,000 people and the email correspondence of a former Albanian president.

Albania responded by severing diplomatic ties with Iran, the first known case of a cyberattack that led to an outcome of this nature. The Iranian hackers then launched a second wave of attacks, disabling systems and deleting information used for border and customs control, including data on everyone who had entered or left Albania during the previous 17 years. The hackers also leaked the names, email addresses, and phone numbers of 600 Albanian intelligence officers; details of an Albanian intelligence operation; and email correspondence between Albanian government ministries and embassies. Albania considered invoking NATO's Article 5 provision for mutual defense—the first time it would have been invoked over a cyberattack—but ultimately decided not to. As of early 2023, Iranian intrusions into Albanian systems were ongoing.[61]

59 Sana Shakil, "Cyber Attacks by Iran Hackers on Rise," *New Indian Express*, March 6, 2022.

60 A leading Iranian opposition group that advocates overthrow of the regime.

61 Andrew Higgins, "A NATO Minnow Reels From Cyberattacks Linked to Iran," *New York Times*, February 25, 2023; Maggie Miller, "Albania Weighed Invoking NATO's Article 5 over Iranian Cyberattack," *Politico*, October 5, 2022; United Against Nuclear Iran, "The Iranian Cyber Threat," (September 2022); Mark Pomerleau, "US Cyber Forces Wrap Up

Espionage (CNE) attacks: In 2011 Iranian hackers breached the Dutch digital certificate authority, DigiNotar. The attack enabled them to spy on the encrypted communications of tens of thousands of Iranian citizens.[62]

In 2011, in "Operation Newscaster," using Twitter, Facebook, and other social media sites, Iranian hackers created a series of phony profiles of journalists who had close ties to government officials. They also set up a fake news site, to gather potentially sensitive information regarding the US–Israeli relationship, the nuclear negotiations then underway with Iran, weapons development programs, and defense issues in general. Over 2,000 computers were compromised, mostly in the United States, including hundreds of current and former senior defense, foreign affairs and other officials. Officials from over 10 US and Israeli defense contractors were also targeted. The attack was only discovered in 2014.[63]

In 2013–2014 an Iranian attack gained control over 16,000 computer systems in the United States, United Kingdom, and elsewhere. Another attack breached the networks of airlines, energy, and defense firms and the intranet of the US Navy and Marine Corps.[64]

Between 2013–2017 Iranian hackers successfully penetrated the computer systems of 320 universities, mostly in the United States, but also some elsewhere, including Israel. The accounts of more than 100,000 academics

Deployment to Albania in Response to Iranian Cyberattacks," *DefenseScoop*, March 23, 2023; Fjori Sinoruka, "FBI: Iranian Hackers Accessed Albanian Systems Over Year Ago," *Balkan Insight*, September 22, 2022; United States Institute for Peace, "Albania Cuts Ties With Iran Over Cyberattack," September 12, 2022.

62 Sue Halpern, "Should the U.S. Expect an Iranian Cyberattack?" *New Yorker*, January 6, 2020.

63 Ellen Nakashima, "Iranian Hackers Are Targeting U.S. officials Through Social Networks, Report Says," *Washington Post*, May 29, 2014; Nicole Perlroth, "Cyberespionage Attacks Tied to Hackers in Iran," *New York Times*, May 29, 2014; Stephen Ward, *Insight Partners*, May 28, 2014; Pierluigi Paganini, "Past and Present Iran-Linked Cyber-Espionage Operations," *InfoSec*, February 20, 2017.

64 Segal, *Hacked World Order*, 151.

were attacked, of which approximately 8,000 were successfully breached, and vast quantities of data and intellectual property were stolen.[65] A further attack against 76 universities in the United States, Israel, and other countries—only uncovered in 2018—sought access to unpublished research and intellectual property.[66]

Another attack, which began in 2014 and continued until its exposure in 2019, used social engineering to steal sensitive information from more than 1,800 accounts of American aerospace and satellite technology firms.[67] Between 2014–2020 a major cyber espionage campaign, reportedly capable of breaching the encrypted messaging systems of Telegram and WhatsApp, targeted Iranian dissidents, opposition groups, and religious and ethnic minorities in Iran, the United States, Canada, the European Union, and more.[68]

In 2015 an Iranian-affiliated attack sought to gain permanent access to the information systems used by members of Germany's Bundestag and their staffs. The attempted infiltration affected the Bundestag's operations for several days and yielded a significant amount of information. Other attacks at the time involved data collection about critical German infrastructure, such as power plants and other utilities.[69]

65 U.S. Department of Justice, "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of The Islamic Revolutionary Guards Corps," Press Release, March 23, 2018.

66 Anthony Cuthbertson, "Iranian Hackers Attack UK Universities to Steal Research Secrets," *The Independent*, August 24, 2018.

67 Rachel Weiner, "Iranian Men Accused of Hacking U.S. Aerospace Companies," *Washington Post*, September 17, 2020.

68 Bergman and Fassihi, "Iranian Hackers Found Way." Particularly prominent targets included the aforementioned Mujahedin-e Khalq (MeK); the Azerbaijan National Resistance organization, which promotes the rights of Iran's large Azeri minority; residents of Iran's restive Sistan and Baluchestan province; Voice of America journalists; and a human rights organization.

69 BBC News, May 13, 2016; Laurens Cerulus, *Politico*, May 22, 2020.

At the height of the negotiations leading to the 2015 nuclear deal, Iranian hackers breached the personal email accounts of the American negotiating team and other US officials, congressional critics of Iran and members of the media. Following the US withdrawal from the agreement in 2018, Iran conducted cyber espionage operations against senior Treasury, State, and Defense Department officials who were involved in the imposition of sanctions. It also stole corporate secrets from 200 infrastructure, aviation, manufacturing, and engineering firms.[70]

In 2016 Iranian hackers conducted a series of attacks against internet service providers and telecommunications firms in the Persian Gulf, which later expanded to government agencies in the United States and 12 European countries. In 2016 the Mabna Institute launched intrusions into the networks of at least 320 universities in 21 countries, including the United States, Australia, Canada, China, Germany, Japan and Israel, and nearly 50 private firms around the world. The attack provided access to confidential research materials.[71]

In 2017 Iranian hackers compromised the login details of 1,000 British members of Parliament and their staffs, over 1,000 Foreign Office officials, and 7,000 police officers. The same hackers targeted the Australian Parliament in 2019, as part of a multi-year cyber espionage campaign, as well as governmental, diplomatic, and military websites in Canada and New Zealand.[72]

In 2018–2019 Iranian-affiliated hackers, posing on LinkedIn as recruiters from Cambridge University and other institutions, sent "job offers" to employees

70 Corey Dickstein, "Military Warns of Iranian Hackers Targeting American Troops With Fake Job Website," *Stars and Stripes*, October 4, 2019; Anderson and Sadjadpour, *Iran's Cyber Threat,* 31, 40; McMillan, "Iranian Hackers Have Hit Hundreds of Companies"; Loudermilk, "Iran Crisis"; Perlroth, "Chinese and Iranian Hackers Renew Their Attacks."

71 Spadoni, "IRGC Cyber-Warfare."

72 Perlroth, "Chinese and Iranian Hackers Renew Their Attacks"; Ewen MacAskill, "Iran to Blame for Cyber-Attack on MPs' Emails – British Intelligence," *The Guardian*, October 13, 2017; Steven Erlanger, "British Parliament Hit by Cyberattack, Affecting Email Access," *New York Times*, June 24, 2017; Ken Dilanian, "Iran-Backed Hackers Hit Both U.K., Australian Parliaments, Says Report," *NBC*, February 28, 2019.

at a variety of Middle Eastern governments, utilities, energy firms and other, designed to lure them into downloading malware. In 2019 the Rana Institute planned and may have carried out an attack on airline and travel booking sites, to gain access to passenger manifests and personal data. Most of the targets were apparently Iranians suspected of anti-regime activities, but some may have been Israeli. Remix Kittens (a.k.a. APT39) also conducted a similar attack.[73]

In 2019 local governments in the United Kingdom, as well as banks and the postal system, were hacked and the identities of thousands of employees stolen, possibly in preparation for more severe attacks on the targets in the future. In another attack, the Elfin group (a.k.a. APT33), which specializes in websites with known vulnerabilities, used spearfishing attacks to gain access to at least 40 governmental and research institutions, as well as commercial and industrial firms in Saudi Arabia, the United States, and elsewhere. The attacks were apparently for purposes of espionage but may have also been in preparation for future destructive ones. In another attack, the Elfin group manipulated or hijacked organizational Domain Name Systems (DNS)[74] to target thousands of employees in Saudi, German, Indian, British, and American oil and gas producers, heavy machinery manufacturers, telecommunications and internet infrastructure providers, and governments.[75]

In 2019 Microsoft blocked 99 websites that had been used by Iranian hackers to conduct multi-year CNE attacks against government agencies, businesses, and individuals in Washington, DC. That year, Iranian hackers also sought to gain access to Pentagon information systems by setting up a website ostensibly designed to serve the needs of military veterans returning to civilian life but which actually downloaded malware onto their computers.

73 King Faisal Center for Research and Islamic Studies, *Iran's Cyberattacks,* 34–35, 40.

74 A core piece of internet infrastructure, which serves as the web's directory or "phone book" and is critical to its operation.

75 King Faisal Center for Research and Islamic Studies, *Iran's Cyberattacks,* 36–38, 41.

US Cyber Command and the Department of Homeland Security grew so concerned over Iranian cyberattacks against American governmental and commercial targets, that they issued a special public warning in mid-2019.[76]

In 2020, shortly after the US-targeted killing of Qassem Suleimani, the head of the IRGC's al-Quds Force, Iranian hackers renewed their attempts to penetrate the US power grid; Refined Kittens (a.k.a. APT33) began a password-spraying campaign to target American electricity, oil, and gas firms;[77] and a related group sought access to similar firms by exploiting vulnerabilities in VPN (virtual private networking) software. The attacks may have been designed to lay the ground for future destructive attacks.[78]

In 2020 Charming Kittens conducted a phishing attack designed to gain access to the emails, cloud storage drives, calendars, and contacts of 20 individuals and organizations. The targets included two Human Rights Watch staffers, a woman's rights activist, an advocate for Lebanese refugees, an American anti-Iranian advocacy group, diplomats, academics, and politicians. In the attack against one of the Human Rights Watch staffers, the person received a fake WhatsApp message from someone who had worked at a Lebanese think tank. In the attack against the American anti-Iranian advocacy

76 Dickstein, "Military Warns of Iranian Hackers"; Ellen Nakashima and Spencer Hsu, "Microsoft Says it Has Found Iranian Hackers Targeting U.S. Agencies, Companies and Middle East Advocates," *Washington Post*, March 27, 2019; Zak Doffman, "U.S. Military Warns Outlook Users to Update Immediately Over Hack Linked to Iran," *Forbes*, July 3, 2019; U.S. Department of Homeland Security, "CISA Statement on Iranian Cybersecurity Threats," *CISA.gov*, January 3, 2020.

77 In password-spraying attacks, the hackers guess hundreds or thousands of common passwords to gain access to user accounts.

78 Andy Greenberg, "Iranian Hackers Have Been 'Password-Spraying' the US Grid," *Wired*, January 9, 2020; Garance Burke and Jonathan Fahey, "AP Investigation: US Power Grid Vulnerable to Foreign Hacks," *Associated Press,* December 21, 2015; Kube, Lee, De Luce, and Dilanian, "Iran Has Laid Groundwork"; Industrial Cyber, "New Dragos report Reveals Iranian Hackers Targeting U.S Power Grid Amid Tensions Between Two Nations," January 13, 2020.

group, United Against Nuclear Iran, the attackers registered a domain that mimicked the real one.[79]

A number of other cyber espionage attacks took place in 2020: A multi-year intelligence collection operation was uncovered that targeted academics, travel and communications firms, government sites, as well as Iranian dissidents and journalists in over 30 countries in North America, Asia, Africa, and Europe; Iranian-affiliated hackers stole "highly protected and extremely sensitive" communications from defense contractors, think tanks, NGOs, universities, and the Afghani and Saudi governments; and Iranian hackers breached the email accounts of several prominent participants at the Munich Security Conference, the preeminent annual gathering of national security officials, as well as of participants at the G20 summit, presumably to gain insights into their strategic thinking. Chancellor Angela Merkel's email was also hacked.[80]

In 2021 two cyber espionage operations targeted 1,200 Iranian dissidents, members of opposition groups, and Kurds in Iran, the United States, United Kingdom, and elsewhere. The first of the two reportedly used an Iranian blog site, Telegram channels, and text messages to lure some 600 victims from seven different countries, into downloading malicious software. The second had actually begun as early as 2007 and spied on dissidents and others in 12 countries, including Sweden, Denmark, the Netherlands, United States, Iraq, and India.[81]

79 Tzvi Joffre, "Iran-Backed Hackers Targeting Activists, Journalists, Politicians – HRW," *Jerusalem Post*, December 5, 2022.

80 Weiner, "Iranian Men Accused of Hacking"; FBI Boston, "FBI Releases Cybersecurity Advisory on previously Undisclosed Iranian Malware Used to Monitor Dissidents and Travel and Telecommunications Companies," September 17, 2020; AP, "Microsoft Says Iranian Hackers Targeted Conference Attendees," October 28, 2020; Kate Connolly, "Russian Hacking Attack on Bundestag Damaged Trust, Says Merkel," *Guardian*, May 13, 2020.

81 Corera, "Iran 'Hides Spyware"; Demboski and IronNet Threat Research and Intelligence Teams, "Analysis of the Iranian Cyber Attack."

In 2021 the same hackers who had posed as recruiters from LinkedIn and Cambridge University three years earlier—seeking to lure targets into downloading malware—now posed as employees of hospitality, medical, airline, and other firms and used Facebook accounts for those purposes. In a clear indication of the scale of the effort required, the hackers conducted ongoing conversations for months at a time with some of their American, British, and European targets.[82] Later that year, Iranian "recruitment" efforts grew particularly dangerous: German, Swedish, and Dutch targets were sent "job offers" with malware attachments, but in this case, the hackers sought sensitive expertise and technology needed to build weapons of mass destruction.[83]

In 2021 Iranian hackers posed as academics from a leading British university to invite experts from the United States and United Kingdom to a conference on Middle Eastern security. Clicks on the "registration link" provided the hackers with access to the victims' computers and with information about their countries' foreign policy, especially regarding the Iranian nuclear issue.[84]

In 2022 Iranian-affiliated hackers successfully penetrated a civilian branch of the US federal government, possibly the Department of Homeland Security, in what may have been intelligence collection in preparation for future destructive attacks. In 2023 Charming Kittens successfully penetrated critical American infrastructure, including multiple seaports and transportation and energy systems. Here, too, the intrusions may have been in preparation for

82 Demboski and IronNet Threat Research and Intelligence Teams, "Analysis of the Iranian Cyber Attack."

83 Tim Stickings, "Berlin Security Service Blames Iran for Cyber Attack on German Companies," *National News*, May 12, 2021; Nakashima and Hsu, "Microsoft Says it Has Found Iranian Hackers."

84 Demboski and IronNet Threat Research and Intelligence Teams, "Analysis of the Iranian Cyber Attack."

future disruptive attacks, possibly in retaliation for US and/or Israeli attacks against Iran.[85]

In 2023 Charming Kittens also impersonated two senior, real-life, experts from Britain's prestigious Royal United Services Institute (RUSI), as a means of establishing contact with nuclear weapons specialists at American think tanks. The phishing attack, which installed malware on the victim's system, was highly targeted, and focused on less than 10 individuals, as part of an effort to gain intelligence on American foreign policy making.[86]

IRGC-affiliated hackers have developed fake mobile apps, similar to Apple Store or Google Play, as a means of disseminating spyware for purposes of surveillance and domestic suppression. The main targets are Iranians, but these apps potentially expose millions of users worldwide to IRGC surveillance. Fake Telegram, Kik, and PlusMessenger apps have been used to exfiltrate data and capture audio and video from 660 largely military targets in the Middle East.[87]

Twenty hacking groups from China, India, North Korea, Pakistan, Russia, and Vietnam, including ransomware operators, spyware vendors, and state-sponsored actors, received command-and-control services from an Iranian affiliated firm in 2023.[88] These services were presumably provided, among other reasons, as a means of gaining intelligence regarding the groups' activities.

Information (CNI) attacks: Iran is increasingly using cyber information operations as a means of achieving its strategic and political objectives.

85 Carly Page, "Iran-Backed Hackers Breached a US Federal Agency that Failed to Patch Year-Old Bug," *Yahoo News*, November 17, 2022; Tim Starks, "An Iranian Hacking Group Went on the Offensive Against US Targets, Microsoft Says," *Washington Post*, April 18, 2023.

86 Derek Johnson, "Iranian Hacking Group Impersonating Nuclear Experts to Gain Intel from Western Think Tanks," *SC Media*, July 6, 2023.

87 Spadoni, "IRGC Cyber-Warfare"; King Faisal Center for Research and Islamic Studies, *Iran's Cyberattacks*, 33.

88 Ionut Arghire, "Iran-Run ISP 'Cloudzy' Caught Supporting Nation-State APTs, Cybercrime Hacking Groups," *Securityweek.com*, August 1, 2023.

These operations are conducted in tens of countries and languages, through numerous news websites, social media, YouTube, and more.[89]

Phony websites produce, propagate, and amplify messaging specifically tailored to American, Latin American, African and Middle Eastern audiences. Iran is portrayed on these sites as a responsible and well-meaning member of the international community that supports the oppressed against an aggressive US-led camp, comprised of Israel, the Gulf states, and Europe. Iran's power is said to stem from the righteousness of its faith, values, and policies, in contrast with Western hypocrisy and American reliance on economic coercion and military force. Special attention is devoted to propagating Shiite theology, the Iranian revolution, and regime policies, as well as support for Shiite movements in the region, Nigeria, Thailand, India, and elsewhere.[90]

In 2011 Iran began an information operation on social media, promoting Iranian positions and those US policies that accorded with Iran's interests, including the need for a nuclear deal, as well as anti-Saudi, anti-Israeli, and pro-Palestinian messaging. In 2018, following the murder of Saudi journalist Jamal Khashoggi, Iran created bots, fake news sites, and Twitter profiles to further disrupt US–Saudi ties and generate international pressure on Saudi Arabia.

In 2018 three major Iranian information operations were exposed. The first, "Ayatollah BBC," had already been underway for about six years. Fake Iranian websites were created to masquerade as some of the major Western radio stations that broadcast in Persian, such as BBC and Voice of America, in order to discredit them, while blocking the real sites on Iranian search

89 Clint Watts, "Rinse and Repeat: Iran Accelerates its Cyber Influence Operations Worldwide," *Microsoft.com,* May 2, 2023; Jack Stubbs and Christopher Bing, "Exclusive: Iran-Based Political Influence Operation – Bigger, Persistent, Global," *Reuters*, August 28, 2018.

90 Tabatabai, *Iran's Authoritarian Playbook*, 3, 6–8, 18; Danny Citrinowicz and Ari Ben-Ami, "The Iranian Information Revolution: How Iran Utilizes Social Media and Internet Platforms to Incite, Recruit and Create Negative Influence Campaigns," *European Eye on Radicalization*, Report 30, July 2022.

engines. Allegedly "independent" news websites, which spread incitement and disinformation about the real ones, were also established. A second operation, which also lasted some six years, consisted of tens or even hundreds of fake news websites and reached a global audience. Each site masqueraded as a local media organization and, in some cases, linked phony headlines to visual and other materials that were unrelated to them. The third operation, launched immediately after the murder of Khashoggi, was directed at a Saudi audience and designed to promote anti-regime sentiment.[91]

In 2019 another information operation was launched, similar in nature to those listed above, but masquerading this time as major print news organizations, including the *Guardian* and the *Independent*. In this case, however, the phony websites included only one fake article at a time, thereby amplifying its impact,[92] compared to the numerous fake articles in the above operations.

In 2019 a large number of fake Twitter accounts in the name of real American citizens, including a number of Republican political candidates, were created to disseminate negative content about Israel and Saudi Arabia. In some cases, the hackers made use of photographs and content taken from the actual accounts of the political candidates, making it difficult to distinguish them from the phony ones. In 2019–2020 millions of people on Facebook, Twitter, Instagram, and YouTube were exposed to a broad-ranging social media campaign critical of the US withdrawal from the nuclear deal, as well as its policies toward Israel, Yemen, and Syria.[93]

91 David Siman-Tov and Ohad Zaidenberg, "Influence Operations: A Combination of Technological Attacks and Content Manipulation," *INSS Special Publication*, March 11, 2021 (Hebrew).

92 Siman-Tov and Zaidenberg, "Influence Operations."

93 King Faisal Center for Research and Islamic Studies, *Iran's Cyberattacks,* 35; Tabatabai, *Iran's Authoritarian Playbook*, 14; Jack Stubbs and Katie Paul, "Facebook Says it Dismantles Disinformation Network Tied to Iran's State Media," Reuters May 5, 2020; Ellen Nakashima, Josh Dawsey, and Matt Viser, "China, Iran Targeting Presidential Campaigns With Hacking

In 2020 the United States seized 92 domains used by the IRGC to conduct information campaigns around the world. Four of the domains posed as ostensibly legitimate news outlets that sought to influence US domestic and foreign policy. The "American Herald Tribune"—a fake Iranian website—actually paid Americans to write articles supportive of Iran's positions, which were then repeatedly referenced, or published in Iranian media, to generate the impression of broad public support for Iran's positions in the United States. In 2020, shortly after the assassination of Qassem Suleimani, the senior leader of the IRGC, Iranian hackers took over the website of a US agency responsible for the distribution of government publications and inserted a picture of a bloody President Trump. Still other information campaigns focused on ethnic and sectarian groups in Iraq, Lebanon, the Persian Gulf, Syria, and Afghanistan.[94]

Iranian information operations have repeatedly sought to promote discord among and between Iran's adversaries. To this end, Iran has used social media in the attempt to further aggravate already existing American racial, socioeconomic, and political tensions, often drawing parallels between them and Iran's own bitter experiences with the United States. In 2020, following the killing of a Black American by a police officer, who pressed his knee against the man's neck until he asphyxiated, President Rouhani claimed that the United States had its knee on Iran's neck, too. Supreme Leader Khamenei and other Iranian leaders repeatedly shared on Twitter their approval of

Attempts, Google Announces," *Washington Post*, June 4, 2020; Craig Timberg, Elizabeth Dwoskin, Tony Romm, and Ellen Nakashima, "Sprawling Iranian Influence Operation Globalizes Tech's War on Disinformation," *Washington Post*, August 21, 2018; Craig Timberg and Tony Romm, "It's not just the Russians Anymore as Iranians and Others Turn Up Disinformation Efforts Ahead of 2020 Vote," *Washington Post*, July 25, 2019; Jay Greene, Tony Romm, and Ellen Nakashima, "Iranians Tried to Hack U.S. Presidential Campaign in Effort that Targeted Hundreds, Microsoft Says," *Washington Post*, October 4, 2019.

94 Kate O'Flaherty, "DoJ Unveils Iran Disinformation Campaign—Seizes 92 Domains Violating U.S. Sanctions," *Forbes*, October 9, 2020; Halpern, "Should the U.S. Expect an Iranian Cyberattack?"; Tabatabai, *Iran's Authoritarian Playbook*, 18, 20.

the Black Lives Matter movement, asserting that the Iranian and American peoples both have been victims of American oppression and hypocrisy; that the United States has freely criticized other countries' human rights practices, while at the same time American ethnic and religious minorities, women, and the LGBTQ community have to fight for their rights. Iranian leaders have also asserted that Europe's silence regarding US human rights violations, all while criticizing Iran's human rights record, manifests Western hypocrisy.

Iran has also repeatedly attempted to influence the American elections. Social media accounts linked to Iran sought to boost the campaign of candidate Bernie Sanders during the 2016 presidential primary elections, because his opponent, Hillary Clinton, was considered more hawkish toward Iran. During the 2018 midterm elections, Iranian hackers impersonated American voters and political candidates on over 7,000 fake Twitter accounts. During the 2020 elections, Iran intervened even more directly in the attempt to sway the outcome in favor of Joe Biden. Iran feared that the reelection of Donald Trump, the outspoken Iran-hawk who had withdrawn from the nuclear deal and imposed severe sanctions on it, could lead to the American pursuit of a regime change in Tehran. Posing as far-right Trump supporters and using email addresses they had gained from a misconfiguration in a voter registration database, IRGC hackers sent out tens of thousands of intimidating emails to Democratic voters in three swing states. "You are currently registered as a Democrat," they warned "and we know this because we have gained access into the entire voting infrastructure. You will vote for Trump on election day, or we will come after you." Further playing on fears that Trump himself had stoked, by claiming that mail-in ballots were subject to fraud, the IRGC hackers also sent out emails with misleading videos designed to undermine voter confidence in the electoral process.[95]

95 Julian E. Barnes and David E. Sanger, "Iran and Russia Seek to Influence Election in Final Days, U.S. Officials Warn," *New York Times*, October 21, 2020; Ellen Nakashima, Amy Gardner, Isaac Stanley-Becker, and Craig Timberg, "U.S. Government Concludes

Iranian efforts to undermine confidence in the integrity of the electoral process continued even after the elections were over. Pioneer Kittens broke into a system that was used by a municipal government to publish election results; the attack could not have affected the outcome, but it could have enabled incorrect reporting of the results, thereby creating the impression that the electoral system had been tampered with and undermining public confidence in it. More ominously, "Enemies of the People," an Iranian-affiliated website, published death threats against elections officials, state governors, the director of the FBI, and a senior cyber official in the Department of Homeland Security, who had refuted Trump's claims of voter fraud.[96]

Iran may have been behind a website called the "Mapping Project," which shows the locations of Jewish organizations and law enforcement and security agencies in Massachusetts. The website threatened the Jewish community

Iran Was Behind Threatening Emails Sent to Democrats," *Washington Post*, October 22, 2020; Ellen Nakashima, Amy Gardner, and Aaron Davis, "FBI Links Iran to Online Hit List Targeting Top Officials Who've Refuted Trump's Election Fraud Claims," *Washington Post*, December 22, 2020; Tabatabai, *Iran's Authoritarian Playbook,* 11, 15–16; National Intelligence Council, "Foreign Threats to the 2020 Federal Elections," (March 10, 2021), 5–7; Miles Parks, "View From the Ground at Washington DC Protests; Misinformation Spreads Online," *NPR*, June 4, 2020; Brian Bennett, "Exclusive: Iran Steps up Efforts to Sow Discord Inside U.S.," *Time*, June 7, 2021; David E. Sanger and Julian E. Barnes, "United States Indicts Iranian Hackers in Voter Intimidation Effort," *New York Times*, November 18, 2021; Phil Muncaster, "US: Iran Was Behind Proud Boys Email Campaign," *Infosecurity Magazine*, October 22, 2020; Lily Hay Newman, "How Iran Tried to Undermine the 2020 US Presidential Election," *Wired*, November 18, 2021.

96 Joseph Menn, "Iran Gained Access to Election Results Website in 2020, Military Reveals," *Washington Post*, April 24, 2023; Christina A. Cassidy and Frank Bajak, "US Cyberwarriors Thwarted 2020 Iran Election Hacking Attempt," *AP*, April 25, 2023; Nakashima, Gardner, Stanley-Becker, and Timberg, "U.S. Government Concludes Iran Was Behind Threatening Emails"; Nakashima, Gardner, and Davis, "FBI Links Iran to Online Hit"; List Tabatabai, *Iran's Authoritarian Playbook,* 11, 15–16; National Intelligence Council, "Foreign Threats"; Parks, "View From the Ground at Washington DC Protests"; Sanger and Barnes, "United States Indicts Iranian Hackers"; Newman, "How Iran Tried to Undermine the 2020 US Presidential Election."

by warning that every organization "has an address, every network can be disrupted." Over two-thirds of the 505 locations shown are police stations or military bases; offices of the Department of Homeland Security, FBI, Secret Service; and government-linked weapons manufacturers.[97]

Iran has reportedly sought to promote domestic dissension also in the United Kingdom. "Free Scotland," an Iranian-affiliated Facebook page promoting Scottish independence, has more than 20,000 followers. "Britishleft.com," one of a number of phony websites, promotes anti-Saudi and anti-Israel messaging. Another site, supposedly in Birmingham, promotes material taken from a state-owned Iranian media network. The cyber information campaign is part of a broader Iranian effort to affect political thinking in the United Kingdom, including through investment in British religious and cultural institutions.[98]

In 2023 the same Iranian hackers who had conducted the information campaign against the 2020 US elections hacked and leaked the names and contact information of more than 200,000 subscribers of Charlie Hebdo, a French satirical magazine. The attack was apparently in response to a series of cartoons critical of Iran's Supreme Leader that the magazine had published at the height of the anti-regime demonstrations in Iran. The hackers used fake Twitter accounts to further amplify the impact of the leaked information.[99]

97 Benjamin Weinthal, "Iran May Be Behind BDS 'Hit List' Targeting Boston Jews – Report," *Jerusalem Post*, March 5, 2023.

98 Charles Hymas, "Iran Targets UK Political System With Fake Websites," *The Telegraph*, June 6, 2021; Paul Stott, *Iranian Influence Networks in the United Kingdom: Audit and Analysis* (Henry Jackson Society, June 2021).

99 Zeba Siddiqui, "Iran Behind Hack of French Magazine Charlie Hebdo, Microsoft Says," *Reuters*, February 3, 2023.