Lt. Gen. (ret) Vincent Stewart, Middle East Media Research Institute (MEMRI)
Special Advisor and Chairman of the MEMRI Board of Advisors
U.S.-Iran Tensions: Implications for Homeland Security

"All men can see these tactics whereby I conquer, but what none can see is the strategy out of which victory is evolved." Sun Tsu

Good morning Chairman Thompson, Ranking Member Rogers, and other distinguished Members of the Committee. I'm honored to appear before you today as Special Advisor and Chairman of the Board of Advisors of the Middle East Media Research Institute (MEMRI), to discuss U.S.-Iran tensions and implications for homeland security. I am proud to be a part of an independent institution which has for over 20 years been at the forefront of documenting and analyzing political, social and intellectual currents in Iran.

As the situation with Iran continues to unfold, I believe it is more important than ever that we pause and put whatever short term actions Iran takes into the longer-term context of Iran's desired end state. We should strive to remember during times of tension that the regime's tactical actions are ultimately a means to an end, and not the ends themselves.

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." Sun Tsu

With that I'd like to start with Iran's **"theory of victory"** or desired end state. Iran believes it is the rightful dominant regional and cultural power, and that the United States and its allies in the region are the impediments to Iran's desired end state. The Iranian government believes they are the victims of US actions and are in fact the rational actor protecting the region and themselves from undue foreign influence. Iran believes it will successfully force the U.S. to leave the region. But the question is, since we're obviously stronger conventionally, how does Iran believe it will accomplish its end state?

Iran understands that its military capabilities will not deter the U.S. from conducting military actions, and that they would certainly be overmatched by our armed forces. Iran has built a capable force that would impose costs on the United States, its allies, its forward staging bases and its interest in the region but cannot militarily match US' capabilities in the long term.

However, Iran views **asymmetric activities** as a viable, low cost means to eject us from the region. Iran's asymmetric warfare can be viewed as a three-legged stool comprising support to malign actors and terrorists, information operations, and a range of cyber activities. All of these components are part of a long-term campaign to make the U.S. cost of staying in the region untenable while eroding support for the U.S. and avoiding the threshold for an overt U.S. military response. Since Iranian military support to terrorists and malign actors can best be viewed through the lens of classified reporting, I'll focus on the second and third legs of the stool and their implications.

Iran's **information operations** are not well understood and target several audiences. The most important is their own domestic population, which the regime seeks to keep united around nationalism and perceived victimhood. Like minded terrorists, militants, and regional religious groups are also a key constituency. Iran's fastest growing audiences are international: Russia and China, and increasingly U.S. allies in the region and abroad. Lastly, I want to highlight that with rise of social media and ease of transmitting messages, the Iranians increasingly see different factions inside the U.S. as information operations targets. That includes building upon the divide between Democrats and Republicans and convincing the American people that we have no interest in the region, that the only thing we can expect from the region is enduring warfare and therefore we should withdraw.

But if those are Iran's information operations targets, what are its messages? Their messages include the following and all support Iran's theory of victory:

- Geography matters, we Iran, have no options of leaving the region, we have a population of 80 million people with a rich 3000+ year history, culture and heritage—we will be here when the Americans leave
- In spite of US propaganda that suggests we are the most de-stabilizing force in the region, we are in fact, the rational actor on the international stage and we conform to international norms of behavior.
- We were abiding by the Joint Comprehensive Plan of Action (JCPOA) agreement, but the United States withdrew from the agreement and imposed economic sanctions to force renegotiations of an agreement that the other parties continue to support.
- Our most capable General was the subject of a targeted assassination while visiting a sovereign country with the attempt to **provoke** an escalation and drag us into war.
- In response to this targeted assassination, we responded in a **proportional** manner and launched missiles at U.S. bases in **self-defense** with the aim of de-escalating the situation.
- Because the missile attack would take place in the sovereign state of Iraq, we alerted the Iraqis, in advance of our missile strikes in compliance with international norms.
- We will ultimately prevail in ejecting the U.S. from the region because we have the moral high ground and you lack the will to persist in the region.

The bottom line on Iranian information operations is this: Anything that gives the regime's narratives a boost is a victory on the path towards Iran's theory of victory. Their three-legged stool of asymmetric warfare is carefully calibrated to make the costs of the U.S. presence high while cultivating an image of being the rational actor and victim. All actions and reactions must be viewed through that lens.

The third leg of Iran's asymmetric efforts are in **cyberspace**. Iran views cyberspace as a vital tool of statecraft and internal security that must be developed in order to undermine enemies and threats to the regime. Iranian doctrine calls for cyber operations as a low cost and often plausibly deniable way to collect information and retaliate against threats. For these reasons Iran often uses proxies to hide cyber operations.

Following the 2010 Stuxnet attack on Iran's uranium enriching capabilities, Iran invested heavily in cyber defenses and capability. Since then it is thought to have carried out some major cyber attacks, including the 2017 attack on Saudi Aramco with the Shamoon virus, following which that network had to be almost completely rebuilt. Also, the 2018 attack on the Italian oil company Saipem, using a version of Shamoon, impacted hundreds of the company's servers as well as personal computers in the UAE, Saudi Arabia, Scotland, and India. Also probed, and hit, were a small dam in update New York in 2016, and the Sands Casino in Las Vegas in 2014.[1] In 2018, the

Department of Justice (DoJ) charged nine Iranians in a widescale cyber-theft campaign, stealing more that 31 terabytes of documents and data from more than 140 American universities and 30 American companies. Previously in March 2016, the U.S. charged seven Iranians for a coordinated campaign of DDoS attacks against 46 companies, mostly in the U.S. financial sector, from late 2011 through mid-2013. In November 2019, Iranian hackers were going after employees at major manufacturers and operators of industrial control systems used by power grids, manufacturing, and oil refineries.[2]

The U.S. Intelligence Community's Worldwide Threat Assessment of January 2019 said that Iran was attempting to build cyber capabilities that would enable attacks against critical infrastructure in the U.S. and elsewhere. It stated that "Iran has been preparing for cyberattacks against the United States and our allies" and that it was capable of "localized, temporary disruptive effects" – including disrupting a large company's corporate networks for days to weeks.[3]

After the January 3 killing of IRGC Qods Force commander Qassem Soleimani, the Department of Homeland Security released on January 4, 2020 a bulletin warning about Iran's "robust cyber program," stating that "Iran is capable, at a minimum, of carrying out attacks with temporary disruptive effect against critical infrastructure in the Unites States" and that "an attack in the homeland may come with little or no warning."[4]

On January 8, Acting DHS Secretary Chad Wolf tweeted that he had "visited the team at Cybersecurity and Infrastructure Security Agency to discuss cyber threats, election security, Iranian cyber capabilities & the impressive work CISA does to protect critical infrastructure. They've been training for years & stand vigilant to respond to any threat against the homeland should one arise."[5] Later that day, the House Homeland Security Committee tweeted that "foreign cyberattacks could pose a serious threat to our nation."[6]

Iran's Cyber Threat Capabilities

On January 6, 2020, the Cybersecurity and Infrastructure Security Agency (CISA) described the Iranian cyber threat: [7]

"Iran and its proxies and sympathizers have a history of leveraging cyber and physical tactics to pursue national interests, both regionally and here in the United States, such as:

- **Disruptive and destructive cyber operations** against strategic targets, including finance, energy, and telecommunications organizations, and an increased interest in industrial control systems and operational technology.
- **Cyber-enabled espionage and intellectual property theft** targeting a variety of industries and organizations to enable a better understanding of our strategic direction and policy-making.
- **Disinformation campaigns** promoting pro-Iranian narratives while pushing anti-U.S. sentiments.
- **Attacks against U.S. citizens and interests abroad** and similar attacks in the Homeland.
- **Unmanned aircraft system (UAS) attacks** against hardened and soft targets."

Official U S Statements

An FBI spokesperson said: "While our standard practice is to not comment on intelligence products, the FBI is aware of the continued possibility that retaliatory actions could be taken against the United States and its interests abroad. [...] While there is no specific or credible threat to the Homeland at this time, we urge the public to be vigilant and report any suspicious activity to law enforcement. As always, we will work with our intelligence and law enforcement partners to gather, share, and act upon threat information."[8]

A January 9 DHS press release about a meeting between Acting Secretary Wolf, CISA, and FEMA stated that "there are currently no specific, credible threats against our homeland." The press release also noted that "Iran has a history of leveraging asymmetric tactics to pursue national interests beyond its conventional capabilities, and its use of offensive cyber operations is an extension of that doctrine. CISA is urging all organizations to assess their cyber readiness and take steps to protect their networks and assets, including adopting a state of heightened awareness, increasing organizational vigilance, confirming reporting processes, and exercising incident response plans."[9]

Roundup of Recent Cyber Incidents with Iranian Involvement[10]

- **January 6, 2020.** The website of the Texas Department of Agriculture was hacked and its homepage replaced with an image of Soleimani and the text "hacked by Iranian Hacker."[11] Texas Governor Greg Abbot tweeted: "Attempted cyber attacks from Iran against Texas agency website are occurring about 10,000 per minute."[12]
- **November 2019**. Microsoft security researchers found that in the last year, an Iranian hacker group carried out "password-spraying attacks" on thousands of organizations, but since October, have focused on the employees of dozens of manufacturers, suppliers, or maintainers of industrial control system equipment and software.
- **October 2019**. The NSA and GCHQ found that a Russian cyberespionage campaign had used an Iranian hacking group's tools and infrastructure to spy on Middle Eastern targets.
- **October 2019**. Iranian hackers targeted more than 170 universities around the world between 2013 and 2017, stealing $3.4 billion worth of intellectual property and selling stolen data to Iranian customers.
- **October 2019**. Iranian hackers conducted a series of attacks against the Trump campaign, as well as current and former U.S. government officials, journalists, and Iranians living abroad.
- **September 2019**. Iranian hackers targeted more than 60 universities in the U.S., Australia, UK, Canada, Hong Kong, and Switzerland in an attempt to steal intellectual property.
- **July 2019.** An Iranian hacking group targeted LinkedIn users associated with financial, energy, and government entities operating in the Middle East
- **July 2019**. U.S. Cybercommand issued an alert warning that government networks were being targeted with malware associated with a known Iran-linked hacking group
- **May 2019.** Iran developed a network of websites and accounts used to spread false information about the U.S., Israel, and Saudi Arabia.

Statements by Iranian Officials on Cyber Issues

May 28, 2019: "The Dejfa ["Digital Fortress"] apparatuses include 10 separate interconnected apparatuses. They are an example of a strong fortress [*dejfa* in Farsi] that primarily guards the country in light of cyberattacks. These apparatuses were created domestically and launched under the command and direction of the MAHER Center [MAHER is the Farsi acronym for Center for Handling and Responding to Cyber Events]. Dejfa is a comprehensive security program that includes a range of security apparatuses. Dejfa identifies a huge part of the threats found online, particularly on the national information network, and neutralizes them. It should be noted that the apparatuses that make up Dejfa are not limited only to identifying and confronting threats on the national information network; they also identify threats in infrastructure, on the Internet, on equipment networks, on cellphones, in industrial equipment and... neutralize them.

"Dejfa is used to discover damage done by malware online, such as bots, identifying the type of malware by anti-virus collection and neutralization. [Using Dejfa] we identify DDoS attacks and neutralize them. Additionally, we analyze the damage that is reported according to international protocols, and confront it. Dejfa also exposes the threats and risks in the protocols of websites. Through Dejfa, users are taught to test the penetrability of software that operates on the Internet, and to search for the level of the strikes against equipment that is used in the country and to confront them. With Dejfa, automatic security assessment is carried out in the apparatuses that operate in cyberspace, and if they are found to be lacking the required security, alerts are issued."[13]

December 13, 2019: Iranian Information and Communications Technology Minister Mohammad-Javad Azari Jahromi tweeted about the thwarting of a cyberattack on Iran: "An organized cyberattack against the Iranian government's electronic systems was identified and thwarted by the Dejfa cyber defense. The attack was carried out as part of the known APT27 attack and was aimed at spying on government data. Servers with the file of the data for spying were identified, and we identified the perpetrators of the attack."[14]

December 9, 2019: Iranian Passive Defense Organization chairman Gen. Gholamreza Jalali said on the subject of a national internet for Iran: "It is true that this [government] support for a national internet [in Iran] came late, but in any event we should be glad that a positive discussion about a national intranet for Iran has found a place also among senior government officials. I personally thank [Iranian President Hassan] Rohani. In my opinion, now is the best time to require all the apparatuses to complete the national internet...

"The Majlis must require the government to complete all phases of the national internet by March 2021. One of the most important areas of the national internet that now has flaws is an Iranian search engine. Its lack was recently felt in the Internet cutoff [during the November 2019 revolt].

"The second priority of the national internet services is an Iranian email [platform]... Likewise, the Majlis must determine the fate of the domestic CDN and DNS...

"This matter of a national internet and its urgency must be clearly explained to public opinion. The establishment of this network is not aimed at cutting off the international internet but is infrastructure that will allow the public to enjoy the fast, quality services of a national internet and at the same time will boost Internet speed in the country. We are striving for independence in cyberspace..."[15]

December 9, 2019: "One of essential things for completing the national intranet is a national metadata [apparatus for searching, cycling, cataloging, and limiting access to data on the Internet]. If we want to provide international-level service, this project must be carried out, because the foundation of most of the new services is in metadata. "[16]

December 8, 2019: Iranian President Rohani said at a Majlis session during the presentation of the 2020-2021 budget: "Since the beginning of the 11th government, broadband capability has been increased 20 times over. This process will continue until we succeed in strengthening the national intranet, such that the public will not need international intranet. Recently, Supreme Leader Khamenei issued an order in this matter. We will monitor the implementation of this order in the Supreme Council of Cyberspace, and our public will notice better conditions in this area..."[17]

December 2, 2019: Iranian Passive Defense Organization Chairman Gen. Gholamreza Jalali said about the need for a national intranet that Iran is "striving for a model of implementing the regime in cyberspace that will be based on our regime's principles and logic... Recent events have proven a number of things on the matter of the national intranet. One of them is that the need for a national network was strongly felt. This network is expected to be independent of a foreign network... "[18]

November 26, 2019: Gen. Jalali said: "Today the area of war is not necessarily military, but is in the arena of culture, economy, cyber, and the creation of science – all are arenas of struggle and supreme effort. Therefore, now is a golden opportunity for the Basij members to enter the various arenas and create victory in all the realms..."[19]

November 24, 2019: IRGC Deputy Commander Gen. Ali Fadavi said: "...The Internet is a means by which America carries out its evil deeds. The Islamic Revolutionary Front will certainly enter into this matter in order to create an internal network for the Internet, such that the enemy will not be able to do evil via the Internet."[20]

November 12, 2019: Gen. Jalali said, in response to a question about whether the reports about the cyberattack on Iran's oil infrastructure by America after Iran downed a U.S. drone were true, that these attacks had been carried out but that they had not impacted Iran's infrastructure.[21]

November 5, 2019: In the Passive Defense Organization, Jalali said: "There is a need to act seriously to inoculate the infrastructure with cybersecurity. In this way, we must show our willingness to the public and to the enemy, to boost public morale and cause the enemy to despair."[22]

October 30, 2019: Iranian Information and Communications Technology Minister Mohammad-Javad Azari Jahromi said at a cyber security work meeting at the Munich Security Conference: "... Iran, having been the target of cyber attacks, has increased its security using Dejfa. With this system, we successfully blocked 33 million cyber attacks last year. Unilaterality and the use of sanctions are threats to international cyber security. The solution for cyber security issues is the use of a multilateral apparatus..."[23]

October 29, 2019: Passive Defense Organization Chairman Gen. Gholamreza Jalali said in an interview on Iran's Channel 2: "The Americans cannot hurt us on the cyber level because we have identified our own weaknesses by conducting four maneuvers in different sectors of energy, transportation, banking, etc... By having a powerful system of defense, we tricked them into our trap."

On the topic of Russian hackers attacking various countries: "**We are indeed seeking cyber defense agreements with friendly countries like Russia, China, India, and Pakistan**. The existence of a national intranet and internal social networks are imperative to our country's security, but the Communications Ministry states that it has not been assigned the specific task of creating a national cyberspace.

"We have five SCADA [Supervisory Control and Data Acquisition] systems that we developed ourselves. We used one for a gas supply network, but there is no consensus about their use for social networks.

"We are fully competitive with foreign [countries] in developing anti-malware [software], and it is imperative that we use anti-malware software that is self-developed for our country's vital networks. We have developed about 200 Iranian cyber products, including switches, routers, and security devices, and if the government gives its support, these products will be superior in quality to foreign products. The country's scientific field has shown how powerful it is."[24]

September 17, 2019: Expediency Council secretary Mohsen Rezaee said at the opening ceremony for the first class of a Basij cyber corps officer development program: "The Americans once fought the nations in the military arena. Now they are moving into cultural, economic, and cyber warfare. The people of the Ashura, with our enterprising and dedicated youth, have rendered American military equipment ineffective, and so the war has been drawn into new arenas."[25]

September 11, 2017 Iranian Army deputy chief of staff Ahmad Reza Pourdastan said at an appreciation ceremony for outstanding communications and technology personnel: "We are facing a complex war. Our capacities in communications and electronic systems are good, and we have turned our ideas into products in a very short time. We have offensive and defensive capabilities in the cyber arena."[26]

October 17, 2017: Iranian Information and Communications Technology Minister Mohammad-Javad Azari Jahromi said: "On October 17, 2017 several Iranian websites were defaced. Fortunately, we identified and contained the issue, which we need to take seriously. The more powerful we become, the more attacks there are. Now Iran is the victim of cyber attacks. Security in Iran's cyber network is very important. We plan to train 10,000 cyber security experts in the next four years."[27]

July 29, 2019: Expediency Council chairman Amoli Larijani met with Song Tao, head of the Chinese International Liaison Department, and said that cooperation in cyber administration and human rights issues is possible between Iran and China. Song Tao said: "China considers Iran a strategic partner and a friend. Despite global developments, we will maintain these relations and they will grow stronger. China is always willing to become active in the region in cooperation with Iran in implementing JCPOA and ensuring peace in the region. We are willing to cooperate in the cyber arena. America's current steps violate international law, but in the future, time will be on the side of Iran and China."[28]

July 23, 2019: Highlights of statements by Passive Defense Organization chairman Gholamreza Jalali: They [the Americans] are openly declaring that they have launched a cyber war against us; therefore it is imperative that we fortify our capacities for cyber-deterrence as much as possible, even though the Americans themselves rate Iran highly in terms of its cyber defenses. The **Americans are more vulnerable to cyber threats than other nations because of their high level of dependence on cyber infrastructure**. This fact has caused some concern due to America's invasive behavior in cyberspace. [29]

July 15, 2019: Basij lieutenant commander Mohammad Hossein Sepehr said at the closing ceremony for the eighth assembly for cyberspace admins: "Khamenei says that 'cyberspace is as important as the Islamic revolution.' The cultural field is part of jihad. If we leave cyberspace we will probably be hit. At this time, the Western faction is the most arrogant in its power in cyberspace, due to its wealth, equipment, and other possibilities. At this time, the most powerful research is in cyberspace... Some view cyberspace as a threat, but it is in fact the greatest opportunity in the Muslim world. According to tradition, power, scope, and speed in communications are signs of the coming of Mahdi. **It is therefore imperative that cyberspace will be under the rule of Shi'ite followers of the twelve imams [Iranian Shi'ite]. Communication sciences must be under the authority of the nation, which in turn is under the authority of Imam Mahdi... Today we must strengthen and bring about the wills through cyberspace**..."[30]

July 7, 2019: IRGC commander Hossein Salami said at the unveiling of the Sepehr 110 Tactical Communications System and its handing over the relevant units: "We can announce that we are at the cutting edge of the following technologies: communication, intelligence, command, and control. We want IRGC communications to be among the most advanced in the world. The cost of science and technology in the field of communications, intelligence, and cyber is very high. We are on the front lines of expanding this knowledge. We intend to act quickly in this field, using our young scientists and engineers. Gradually, our enemies are coming to understand out true power. Our enemies are focused on economic warfare, psychological maneuvers, and political pressure in an effort to shake the will of the Iranian people to continue on the path of honor."[31]

June 27, 2019: An article by Abu Al-Fazel Nia, cultural advisor at the Iranian Embassy in Syria, stated: "At the height of the media coverage of the situation in the Gulf and the possibility of a U.S.-Iran war, Iran announced that it had successfully uncovered the CIA's espionage networks – in Iran and some countries of the region and the world, exposing American spies. It is possible that this news did not get much attention because the public was too occupied with Trump's changeable position towards Iran, and due to the American effort to draw attention away from its defeat in the cyber arena by Iran's cyber champions; This shows that Iranians are superior to Americans in the virtual arena. This Iranian accomplishment is a victory for the resistance – which is not only an armed resistance, but an array of resistance across all aspects of life; The world is trying to mislead the public about Iran's technological capabilities."[32]

June 17, 2019: Supreme National Security Council secretary Ali Shamkhani said: "Alongside the economic war and the intelligence war, America is carrying out cyber attacks against Iran and many countries. We examine and look at these threats by cooperating and having close ties with our partners, and we have activated protective measures against them.

"A while ago, one of the CIA's most complex cyber networks was exposed and damaged by the Iranian intelligence apparatus. Due to the cooperative anti-espionage network Iran is part of, alongside many other world countries, we shared information about the American network with our partners, which led to the uncovering and collapse of a network of CIA intelligence outposts and the arrests of several spies, who were punished in different countries. The Americans called Iran's action an embarrassing failure."[33]

Conclusions/Assessments

A June 25, 2019 assessment of Iran's cyber power by the Center for Strategic and International Studies Senior VP James Andrew stated that Iran's cyber operations are conducted primarily by the IRGC, the Basij, and Iran's Passive Defense Organization. According to the assessment, the IRGC is behind a series of incidents against American targets, Israeli critical infrastructure, Saudi Arabia, and other Gulf states. The Basij manages what its leaders say are 120,000 cyberwar volunteers; while this number is probably exaggerated, the Basij uses its connections in universities and religious schools to recruit a proxy hacker force. The Passive Defense Organization is responsible for protecting Iran's infrastructure. There is also Iran's Supreme Council of Cyberspace, comprising senior military and intelligence officials.

The assessment adds that while Iran has probed U.S. critical infrastructure for targeting purposes, it is not clear how successful an attack would be. The kind of massive denial of service attacks it carried out against major banks in 2011-2013 would not be so effective today, while "the most sophisticated kinds of cyberattack (such as Stuxnet or the Russian actions in the Ukraine) are still beyond Iranian capabilities." However, poorly defended targets in the U.S., such as smaller banks or local power companies, or poorly secured pipeline control systems, are vulnerable. " What stops Iranian action," he said, "is not a shortage of targets but rather questions about the utility of such attacks."[34]

Other past attacks that would not be as successful today involved using malicious software to wipe data, or potentially hijacking crucial machinery, as Iranian hackers attempted to do with the New York state dam in 2013.[35]

Immediately after Soleimani's killing, Jon Bateman, a former Defense Intelligence Agency analyst on Iran's cyber capabilities and now a cybersecurity fellow for the Carnegie Endowment for International Peace, said, "At this point, a cyberattack should be expected."[36] However, Hoover Institution at Stanford fellow Jaquelyn Schneider stated: "In an already dangerously volatile situation, the United States should not focus unwarranted attention on potential cyberattacks by Iran." Doing so, she added, "is a distraction from the real risk of escalation -

highly alert military forces in the region inadvertently firing at one another or crossing redlines toward all-out war."[37]

Implications

The question is not whether the Iranians have the capability to attack our public and private sector institutions, but when, where and how we will respond?

The Iranians are not as capable as the Russians or the Chinese. But they have expressed their intent to develop both offensive and defensive capabilities. They are partnering with other countries to learn, share and counter our interest. They have demonstrated an ability to conduct attacks incurring costs to private U.S. companies and foreign entities in the multi-million dollar range. They will include cyberspace operations as a key component of their asymmetric response to the killing of Soleimani. What makes this foreign threat so unique, is that it is the one area where the U.S. government is essentially telling the U.S. private sector to "fend for yourselves." We need a national level strategy on protection of U.S. companies from foreign cyber threats touching on everything from information sharing to insurance. Having spent the last two years in the private sector after decades in public service, I am consistently struck by how little our private sector leaders understand the threat or what actions they should take in response. We need a common understanding of what an attack and war in cyberspace looks like. We need increased emphasis on public-private partnership to achieve "collective defense", and we need increased emphasis on educating the populace on the real threat from cyberspace activities.

I look forward to your questions.

[1] Npr.org/2020/01/09/794816793/federal-authorities-warn-of-irans-cyber-threat-capabilities, January 9, 2020.

[2] Zdnet.com/article/hard-disk-wiping-malware-phishing-and-espionage-how-irans-cyber-capabilities-stack-up/, January 7, 2020; Forbes.com/sites/kateoflahertyuk/2020/01/06/the-iran-cyber-warfare-threat-everything-you-need-to-know/#29ba0b3015aa, January 6, 2020.

[3] https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

[4] Dhs.gov/sites/default/files/ntas/alerts/20_0104_ntas_bulletin.pdf, January 4, 2020.

[5] Twitter.com/DHS_Wolf/status/1214948930070482951, January 8, 2020.

[6] Twitter.com/HomelandDems/status/1215018179828822018, January 8, 2020.

[7] Cisa.gov/insights, January 6, 2020.

[8] Thehill.com/policy/cybersecurity/477434-fbi-dhs-issue-bulletin-warning-of-potential-iranian-cyberattacks, January 8, 2020.

[9] Dhs.gov/news/2020/01/09/acting-secretary-wolf-receives-updates-fema-and-cisa-traveling-honduras, January 9, 2020.

[10] Csis.org/programs/technology-policy-program/significant-cyber-incidents, accessed January 9, 2020.

[11] Thehill.com/policy/cybersecurity/477408-texas-department-of-agriculture-website-featured-pro-iran-image-after, January 8, 2020.

[12] Twitter.com/GregAbbott_TX/status/1214955296721903618, January 2, 2020.

[13] YJC.ir/fa/news, May 28, 2019.

[14] https://twitter.com/azarijahromi/status/1206071513222467585

[15] Farsnews.com, December 9, 2019.

[16] Farsnews.com, December 9, 2019.

[17] President's website, President.ir/fa/112698, December 8, 2019.

[18] https://www.memri.org/tv/irgc-general-gholamreza-jalali-head-iran-civil-defense-organization-waze-israeli-tools-demonstrations-need-intranet; https://www.shahrekhabar.com/political/157536384011529

[19] IRNA, November 26, 2019.

[20] ISNA.ir, November 24, 2019.
[21] ISNA.ir, November 12, 2019.
[22] Farsnews.com, November 11, 2019.
[23] Farsnews.com, October 30, 2019.
[24] ISNA.ir, October 29, 2019.
[25] Tasnimnews.com, October 17, 2019
[26] Tasnimnews.com, September 11, 2017
[27] Tasnimnews.com. 2017
[28] Tasnimnews.com, July 29, 2019.
[29] ISNA.ir, July 23, 2019
[30] Farsnews.com, July 15, 2019
[31] Tasnimnews.com, July 7, 2019
[32] Alwatan.sy/archives/202919, June 27, 2019.
[33] Mehrnews.com, June 17, 2019.

[34] Csis.org/analysis/iran-and-cyber-power, June 25, 2019.
[35] Washingtonpost.com/technology/2020/01/03/cyber-attack-should-be-expected-us-strike-iranian-leader-sparks-fears-major-digital-disruption, January 3, 2020; Washingtonpost.com/politics/2020/01/06/iran-can-use-cyberattacks-against-us-thats-not-nearly-bad-it-sounds, January 6, 2020.
[36] Washingtonpost.com/technology/2020/01/03/cyber-attack-should-be-expected-us-strike-iranian-leader-sparks-fears-major-digital-disruption, January 3, 2020.
[37] Washingtonpost.com/politics/2020/01/06/iran-can-use-cyberattacks-against-us-thats-not-nearly-bad-it-sounds, January 6, 2020; Nytimes.com/2020/01/07/opinion/iran-cyber-attack-hacking.html, January 7, 2020.