Thomas S. Warrick
Atlantic Council Non-Resident Senior Fellow
January 15, 2020, "U.S.-Iran Tensions: Implications for Homeland Security"

Mr. Chairman, Ranking Member Rogers, members of the House Committee on Homeland Security, thank you for the opportunity to testify today on implications of current U.S.-Iran tensions on homeland security.

In the morning hours of Wednesday, January 8, 2020, Iraqi time, the Iranian Islamic Revolutionary Guards Corps (IRGC) fired 22 surface-to-surface missiles at two Iraqi airbases, Al-Asad and Irbil, killing no one. According to the New York Times this past Sunday, if that attack had killed any Americans, the Pentagon would have put in front of President Trump a set of retaliatory options that included strikes on an Iranian naval vessel and cyberattacks "to partly disable Iran's oil and gas sector."

Would the United States oil and gas industry have been ready for an Iranian cyberattack that would likely have followed?

That is a hypothetical question, but the next one is real. While Americans celebrated Thanksgiving, someone hit Iran with a massive cyberattack: publicly disclosing 15 million Iranian bank debit card numbers on a social media site. On Wednesday, December 11, Iran's telecommunication minister—who previously shrugged off U.S. cyber retaliation for the September 14 Iranian attack on a Saudi oil facility—made the rare admission this was "very big."

After first saying the attack was an inside job, Iran said on December 11 that a nation-state carried it out.

Are we confident that all the banks and credit card companies in the United States are ready to defend themselves if Iran tries to hack into the names and card numbers of millions of Americans?

Since the December 27 killing of an American citizen at an Iraqi military base outside Kirkuk, a lot of attention has rightly been paid to the possibility of a shooting war between Iran and the United States. However, for more than a decade, Iran and the United States have been engaged in a campaign in cyberspace that affects the U.S. Homeland. That campaign is now expanding into other arenas as well. Iran's campaign deserves more attention from the American people and the U.S. Government because it requires us to look at possible strategic gaps in our defenses. For example, while most Federal government computers are protected, U.S. civilian cyber defenses are uneven.

This campaign fits into a larger strategic picture that we can discuss during the question and answer session. Today I will go quickly through the four ways that Iran threatens the Homeland. I would like to draw the Committee's attention to three preliminary points about cyberattacks specifically. I will then focus on what I call Iran's peculiar sense of symmetry, which helps

explain much of Iran's logic in its campaigns against us. Finally, I would like to respectfully suggest some areas where the Committee may be able to help the United States better secure itself from Iran's efforts to target us, especially in cyberspace.

Four Ways Iran Threatens the United States

There are four possible attack vectors that Iran could use to target the United States: terrorism, cyberattacks, disinformation, and influence operations.

1. **Terrorism is unlikely but possible, at least in the short term.** The last state-sponsored attempted terrorist attack on U.S. soil was in 2011, when an extremely small number of IRGC Qods Force (IRGC-QF) officers, including Abdul Reza Shahlai, tried to assassinate the Saudi Arabian ambassador, Adel Al-Jubeir, in a Washington restaurant. The plot was worked through Mansour Arbabsiar, who was arrested by the FBI in 2011 when his flight between Mexico City and Amsterdam landed at New York's John F. Kennedy airport. Arbabsiar pled guilty and cooperated with authorities in helping obtain evidence against other IRGC officers involved in the plot. Arbabsiar is now serving a 25-year sentence in Federal prison in Marion, Illinois. U.S. law enforcement officials long tried to bring Abdul Reza Shahlai to justice, most recently on December 5, 2019, by offering a $15 million reward for information leading to the disruption of his fund-raising and spending networks. He was reportedly the target of a separate strike in Yemen the night of January 2-3. Although it is unlikely the Houthis in Yemen, who get resources and aid from Shahlai and the IRGC-QF, would turn him over, the United States should continue to bring him to justice.

   Iran also can call on proxy groups like Lebanese Hizballah. On December 3, 2019, Ali Kourani was sentenced to 40 years in prison for being a sleeper operative for Hizballah's terrorist arm, the Islamic Jihad Organization.

2. **Cyber-threats from Iran are certain, and ongoing.** DHS's Cybersecurity and Infrastructure Security Agency (CISA) put out a statement by Director Chris Krebs in June and elevated it to an alert on January 6 after the January 2 strike on Qasim Soleimani. DHS released a National Terrorist Advisory System (NTAS) Bulletin on January 4. DHS and the FBI have also released a Joint Intelligence Bulletin to state and local law enforcement. I will focus on Iran's cyber threats in a moment, but the extent to which the Iranians are improving in this area should be a concern.

3. **Disinformation operations.** Iran has used disinformation operations against the United States, spreading false propaganda that has included the outrageous idea that the United States supported ISIS. A State Department Inspector General report said that in 2016, one-third of the Iraqi public held this view. Iranian disinformation was the chief reason.

4. **Influence operations.** Facebook and Twitter have found thousands of social media accounts who looked liked regular users and independent organizations, but were in fact linked to the Iranian government.

Three preliminary points about cyberattacks

Mr. Chairman, permit me to go back to cyberattacks.

First, when Iran retaliates for attacks against it, Iran and its allies consider the United States, Israel, and Saudi Arabia as responsible for each other's attacks. Iranian proxies held the United States responsible for a strike conducted by the Israelis. To be sure, the United States holds Iran responsible for the actions of Iran's proxies.

Second, in recent months, the Trump Administration has decided that sanctions and cyberattacks are their go-to tools. After the September 14 kinetic attack on a Saudi oil facility, the Trump Administration searched for a "cyber silver bullet." President Trump was reportedly "reluctant to widen the conflict in a region he has said the United States should leave." And, as I noted earlier, a cyber attack was one of the options if the Iranians had killed anyone at Al-Asad or Irbil on January 8.

This leads me to my third preliminary point. The implication that cyberattacks are somehow safer for the United States than kinetic attacks is dangerous. The cyber defenses of Iran's likely targets in the United States are uneven. More needs to be done to prepare the American people for Iranian cyber retaliation.

Iran's peculiar sense of symmetry

This leads me to my most important point: When it comes to the United States, Iran's government follows a peculiar sense of symmetry. When the United States does something to Iran, Iran tends to respond—not exactly in the same way, but the symmetry is almost always there.

This applies across the board, in both kinetic attacks and in cyberspace. Look at what Iran said and did after the January 2 strike against Islamic Revolutionary Guards Corps Qods Force (IRGC-QF) Major General Qasim Soleimani. The next day, Iranian Supreme Leader Khamenei made an unusual appearance at the Iranian Supreme National Security Council and gave them a written order that Iran "strike America directly and in exact proportion to the attack," as two sources told the New York Times.

Consider the September 14 Iranian attack on Saudi oil facilities at Abqaiq: Starting in May 2018, "maximum pressure" U.S. sanctions reduced Iran's oil exports. Iran thinks it is defending itself against economic warfare waged by the United States. After Iran tried for a year to get Europe to ease the pressure, Iran showed it could reduce U.S. allies' ability to export oil, first in May and June with attacks on tankers and a Saudi pipeline, then with the Abqaiq attack that halved Saudi oil exports.

Another symmetry: On July 4, Britain seized an Iranian tanker violating international sanctions. On July 19, Iran seized a British tanker. On August 15, Gibraltar authorities released the Iranian tanker. On September 27, Iran released the British tanker.

Iran's sense of symmetry is more pronounced in cyberspace. In 2013, Iran developed a cyberattack capability after the "Stuxnet" malware that targeted Iran's Siemens industrial control systems (ICS) came to light in June 2010. From Stuxnet's discovery until Iran's first ICS attack was three years.

On July 30, 2012, new U.S. sanctions targeted Iranian banks. Two months later, Iran ramped up denial of service attacks whose main targets were—U.S. banks.

In August 2012, Iran's surprise "Shamoon" attack deleted 35,000 Saudi Aramco hard drives and was described as "the biggest hack in history." What got less publicity is that in early 2012, malware later dubbed "Wiper" deleted data on Iranian Oil Ministry and National Iranian Oil Company computers.

The symmetry can be positive: When the Iran nuclear deal was in force, Iranian cyberattacks appeared to drop. This comes from anecdotal evidence, because U.S. companies are not required to report Iranian cyber attacks to the Department of Homeland Security.

When the Trump Administration began its 2018 "maximum pressure" campaign, Iranian cyberattacks increased within 24 hours.

On June 20, 2019, after Iranian attacks on civilian tankers, President Trump retaliated by cyberattack. Private US businesses noticed a further increase in Iranian cyberattacks.

This leads to three important points: Over time, Iran has both ***improved*** its cyber capabilities and ***reduced*** its response time. What took Iran three years to respond to in 2010, and six months to respond to now in 2012, is now down to days and hours.

Additionally, the United States also needs to recognize that Iran is capable of ***strategic surprise.*** Iran achieved strategic surprise with the precision of its kinetic attack against Abqaiq in September 2014, and the apparent precision in hitting targets on January 8 at Al-Asad and Irbil—all without killing anyone. Iran could achieve strategic surprise in cyberspace, and we would not know it until they hit us.

Before I go on to discuss what we should do, I want to make one point clear. Iran's sense of symmetry doesn't mean that if we stopped what we're doing, Iran would stop being a threat to the United States and our allies. Iran would still continue to harbor its nuclear ambitions and, more importantly, it would continue its malign behavior that is de-stabilizing the region, including being a threat to Israel and other U.S. allies. We can discuss this more in the question and answer session, but Iran's strategic goals have never been more clear than they are now, after the January 2 strike that killed Qasim Soleimani.

What US policymakers should do

Mr. Chairman, let me turn to what the United States should do to address the threats to the Homeland from Iran. I will focus here on Iran's most active threat to our the cyber defenses.

Most Federal government computers are protected, but U.S. civilian cyber defenses are uneven. Iran's previous civilian targets included "aerospace, defense, and petrochemical companies," local government, universities, and a business owned by a prominent American supporter of Israel.

On June 22, Chris Krebs, the director of DHS cybersecurity warned of a "rise in malicious cyber activity ... by Iranian regime actors and proxies." He warned of increasing Iranian use of "wiper" attacks and Iranian efforts "to steal data and money." He renewed this warning earlier this month.

Normally, when U.S. policymakers consider kinetic strikes, they activate plans to notify and protect military and civilian personnel and facilities. The same logic should apply for cyberattacks, but it doesn't.

First, responsibility for offense and defense is divided. Cyber Command and the National Security Agency handle military offense and defense, but the FBI, DHS, and—notably—the private sector handle civilian defense. While there is coordination, they don't all go to the same meetings or have access to the same information.

Second, notification of the private sector in advance of cyberattacks by the United States or our allies is not feasible because too many people would have to be notified. If Iran's retaliation is fast, decentralized, or has good opsec, the private sector will get no warning.

Normally, the threat of Iranian cyber retaliation would lead the President and his top officials to have a frank conversation with the American people about why cyberattacks against Iran are necessary and why Americans should increase their cyber defenses, roughly analogous to the 1950s "civil defense" campaign.

However, drawing attention to the risks of cyberattacks against Iran would undercut the President's goal not to be seen heading into another Mideast conflict. Yet the best defense is to say, publicly and in multiple channels, that the American people need to do more to defend themselves against cyber threats from Iran and elsewhere.

DHS's campaign since January 3 of repeating earlier warnings, issuing an NTAS bulletin, and issuing cybersecurity alerts are all welcome developments. My concern is that these warnings will reach cybersecurity experts and people like this panel who follow threats from Iran very closely, but that the American people and smaller American businesses will not. Cyber operators are looking for the unlocked door.

This starts with the basics: (1) Update your software. (2) Install anti-virus software. (3) Use two-factor authentication where you can. (4) Watch out for phishing emails. (5) And most importantly, educate yourself to resist efforts by our adversaries to sow division among Americans. Congress should give thought to how we educate both our young people in school and ourselves as adults. Cyber defense is a lifelong enterprise.

Lower level warnings, like the CISA director's January 4 statement, will not be enough to deter severe criticism from the American people if Iran achieves strategic surprise like Iran's 2012 Shamoon attack or the recent Abqaiq attack.

The United States and its allies should not "do nothing" in response to attacks like Abqaiq. Nor should we cease all measures that oppose Iran's destabilizing actions.

However, because of Iran's peculiar sense of symmetry, the Trump Administration needs to do more to prepare the American people to defend against Iranian cyber retaliation. Whoever was behind the exposure of 15 million Iranians' debit card numbers, the Iranians will be motivated to retaliate in kind. A possible cyber attack to partially disable the Iranian oil and gas sector could put America's oil and gas sector at risk of a comparable attack.

Iran has shown us, twice, that the IRGC has improved its kinetic capabilities. It has shown us over the past ten years it has improved its cyber capabilities. It's incumbent on the U.S. Government to work more closely with the public and the private sector to improve U.S. cyber defenses. Iran will continue to be a threat for the foreseeable future.

I would be happy to address any questions and to go into the strategic issues that we haven't been able to cover so far today.

Thomas S. Warrick is a Nonresident Senior Fellow at the Atlantic Council. He worked Iraq and Iran issues for the State Department from 1997-2007 and was the Department of Homeland Security's senior Iran expert from 2007 until June 2019.