U.S.-IRAN TENSIONS: IMPLICATIONS FOR HOMELAND SECURITY

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

JANUARY 15, 2020

Serial No. 116–57

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
41–269 PDF WASHINGTON : 2020

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
CEDRIC L. RICHMOND, Louisiana
DONALD M. PAYNE, JR., New Jersey
KATHLEEN M. RICE, New York
J. LUIS CORREA, California
XOCHITL TORRES SMALL, New Mexico
MAX ROSE, New York
LAUREN UNDERWOOD, Illinois
ELISSA SLOTKIN, Michigan
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
YVETTE D. CLARKE, New York
DINA TITUS, Nevada
BONNIE WATSON COLEMAN, New Jersey
NANETTE DIAZ BARRAGÁN, California
VAL BUTLER DEMINGS, Florida

MIKE ROGERS, Alabama
PETER T. KING, New York
MICHAEL T. MCCAUL, Texas
JOHN KATKO, New York
MARK WALKER, North Carolina
CLAY HIGGINS, Louisiana
DEBBIE LESKO, Arizona
MARK GREEN, Tennessee
VAN TAYLOR, Texas
JOHN JOYCE, Pennsylvania
DAN CRENSHAW, Texas
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina

HOPE GOINS, *Staff Director*
CHRIS VIESON, *Minority Staff Director*

CONTENTS

U.S.-IRAN TENSIONS: IMPLICATIONS FOR HOMELAND SECURITY

Wednesday, January 15, 2020

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The committee met, pursuant to notice, at 10:03 a.m., in room 310, Cannon House Office Building, Hon. Bennie G. Thompson [Chairman of the committee] presiding.

Present: Representatives Thompson, Jackson Lee, Langevin, Richmond, Correa, Torres Small, Underwood, Slotkin, Green of Texas, Titus, Barragán, Demings; Rogers, King, Katko, Higgins, Green of Tennessee, Joyce, Crenshaw, Guest, and Bishop.

Chairman THOMPSON. The Committee on Homeland Security will come to order.

The committee is meeting today to receive testimony on "U.S.-Iran Tensions: Implications for Homeland Security." Without objection, the Chair is authorized to declare the committee in recess at any point.

Good morning. Today the committee is meeting to examine the Homeland Security implications of the recent escalation in U.S.-Iran tensions in the wake of the killing of Qassem Soleimani. Iran and Iranian-linked terrorists have shown a capability and willingness to conduct terrorist attacks against the United States and our allies and interests abroad. Clearly the escalation of tensions between the United States and Iran could have dire consequences for the security of the homeland.

More broadly, the suspension of U.S.-led counterterrorism efforts against ISIS in the region ostensibly, in order to focus on the threat from Iran and its proxies may allow ISIS to reconstitute in unsecured areas of Iraq and Syria. This would dramatically undermine the fight against ISIS and make U.S. interests abroad and home less safe.

As Members of Congress we have an obligation to do everything in our power to protect our constituents by defending the Nation from physical attacks, cyber attacks and influence campaigns designed to undermine our democracy and sway public opinion in favor of Iran, or its friends.

I am deeply concerned that President Trump has no strategy and his administration has failed to plan adequately for addressing the Homeland Security consequences that might follow military actions in Iran. The administration must immediately put forward a measured comprehensive strategy that accounts for potential threats to the homeland from Iranian actors and their proxies.

As part of that strategy, the Department of Homeland Security must ensure it is prepared for all contingencies related to the escalation in U.S.-Iran tensions. I look forward to a frank discussion today about what the strategy should be. I am particularly interested in understanding how Iran could use its relatively sophisticated cyber capabilities against State and local governments and critical infrastructure to extract revenge for the death.

We need to understand whether potential targets are prepared to defend against Iranian cyber threats and what the Federal Government can do to help them if they are not. Although there have been no specific threats to the critical infrastructure, escalation of tensions with any adversary demands that we take stock of all the current measures we employ to defend ourselves. This is particularly true in the case of Iran, a country that is unpredictable in its responses and hide behind proxies and sympathizers to do its dirty work.

Toward that end I would be remiss if I did not note that the Chemical Facilities Anti-Terrorism Standards Program is set to expire in April. Although the House has begun work on reauthorizing this important antiterrorism program, the Senate has not. At this point it is unclear if the Senate intends to work with the House to reauthorize the program. I urge the Senate to begin work on this National security priority. It would be irresponsible to allow the program to lapse at this time.

Finally, in recent weeks we have seen an uptick in Iran's influence activity on social media. I do not need to tell anyone here that it is an election year and influence activity is bound to increase. Given the committee's election security work, I am concerned Iran might escalate its influence activities as we approach the election and what more the Federal Government and its private-sector partners should be doing to counter Iranian messaging.

We need to be prepared to confront and defend against Iran's influence efforts and ensure the integrity of our democracy and our most sacred institutions. We are fortunate to be joined by witnesses with vast experience with the Department of State, Defense, and Homeland Security as well as expertise in matters related to Iran.

I look forward to a productive discussion today and remain committed to ensuring this committee does its part to help secure the homeland from threats posed by Iran, its proxies, or any other who would seek to do to harm to Americans.

The Chair now recognizes the Ranking Member of the full committee, the gentlemen from Alabama, Mr. Rogers, for an opening statement.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

JANUARY 15, 2020

Today, the committee is meeting to examine the homeland security implications of the recent escalation in U.S.-Iran tensions in the wake of the killing of Qasem Soleimani. Iran and Iranian-linked terrorists have shown a capability and willingness to conduct terrorist attacks against the United States and our allies and interests abroad. Clearly, the escalation of tensions between the United States and Iran could have dire consequences for the security of the homeland. More broadly, the suspension of U.S.-led counterterrorism efforts against ISIS in the region, ostensibly in order to focus on the threat from Iran and its proxies, may allow ISIS to reconsti-

tute in unsecured areas of Iraq and Syria. This would dramatically undermine the fight against ISIS and make U.S. interests abroad and home less safe.

As Members of Congress, we have an obligation to do everything in our power to protect our constituents by defending the Nation from physical attacks, cyber attacks, and influence campaigns designed to undermine our democracy and sway public opinion in favor of Iran or its friends. I am deeply concerned that President Trump had no strategy and his administration has failed to plan adequately for addressing the homeland security consequences that might follow military action in Iran. The administration must immediately put forward a measured, comprehensive strategy that accounts for potential threats to the Homeland from Iranian actors and their proxies.

As part of that strategy, the Department of Homeland Security must ensure it is prepared for all contingencies related to the escalation in U.S.-Iran tensions. I look forward to a frank discussion today about what that strategy should be. I am particularly interested in understanding how Iran could use its relatively sophisticated cyber capabilities against State and local governments and critical infrastructure to exact revenge for the death of Soleimani. We need to understand whether potential targets are prepared to defend against Iranian cyber threats, and what the Federal Government can do to help them if they are not. Although there have been no specific threats to critical infrastructure, escalation of tensions with any adversary demand that we take stock of all the current measures we employ to defend ourselves. This is particularly true in the case of Iran, a country that is unpredictable in its responses and hides behind proxies and sympathizers to do its dirty work.

Toward that end, I would be remiss if I did not note that the Chemical Facilities Anti-Terrorism Standards Program is set to expire in April. Although this House has begun work on reauthorizing this important anti-terrorism program, the Senate has not. At this point, it is unclear if the Senate intends to work with the House to reauthorize the program. I urge the Senate to begin work on this National security priority. It would be irresponsible to allow the program to lapse at this time.

Finally, in recent weeks, we have seen an uptick in Iran's influence activity on social media. I do not need to tell anyone here that it is an election year, and influence activity is bound to increase. Given this committee's election security work, I am concerned Iran might escalate its influence activities as we approach the election and what more the Federal Government and its private-sector partners should be doing to counter Iranian messaging. We need to be prepared to confront and defend against Iran's influence efforts and ensure the integrity of our democracy and our most sacred institutions.

We are fortunate to be joined by witnesses with vast experience with the Departments of State, Defense, and Homeland Security and expertise in matters related to Iran. I look forward to a productive discussion today and remain committed to ensuring this committee does its part to help secure the homeland from threats posed Iran, its proxies, or any others who would seek to do America harm.

Mr. ROGERS. Thank you, Mr. Chairman. Iran has been escalating tensions in the Middle East for decades. Since the Nuclear Deal was signed, Iran's malign activities have only increased.

The $100 billion in assets released by the Obama administration helped Iran enhance the manpower and capability of its terrorist proxies. It helped Iran to conduct vicious cyber attacks on private industry and allied nations. It enabled them to grow their missile stockpiles and improve their lethality.

Six months after it signed the JCPOA, Iran conducted ballistic missile test with missiles carrying the inscription, "Israel should be wiped off the Earth". It is clear that the Obama-era policies of appeasement did not work. The President was right to take the United States out of the JCPOA and reimpose sanctions.

The President understood that the JCPOA was not going to contain Iran. That flawed deal was doing nothing to end the very clear and direct threat the Iranian regime poses to the United States, Israel, and the rest of our allies. For over a decade, Iran has funneled money, terrorists, and advanced weapons to its proxies in Iraq, Syria, and Lebanon, who used them to attack U.S. troops and Israeli citizens.

In doing so, Iran is responsible for the deaths of over 600 Americans. The latest American murdered at the hands of Iran was a civilian contractor and father of 2 young children in California. Fortunately, the President took decisive action to eliminate the brutal terrorist primarily responsible for his death and the deaths of thousands of others.

Qassem Soleimani was sanctioned as a terrorist by the United Nations and the Obama administration. For over 20 years he lived at IRGC's Quds Force, a foreign terrorists' organization. Soleimani was not visiting Baghdad because it was a great holiday destination. He was there with—as some peace envoy—he was not there as some peace envoy. He was there to meet with a leader of a terrorist group to plan more attacks on Americans.

The President used the law and his Constitutional authority as commander-in-chief to eliminate this terrorist mastermind before he could kill again. For the first time in years Iran received the message that there will be no real consequences should they continue to threaten—that there will be real consequences should they continue to threaten the United States and our allies.

I hope Iran understands this message and finally ends their malicious and destabilizing actions in the Middle East. I also hope that the Iranian regime understands that the United States will not hesitate to defend our homeland against any threat that they advance.

For years the Department of Homeland Security, FBI, and other law enforcement partners have kept close watch on Iran's intentions and its capability to strike our homeland. The threat from Iran is real. We know they continue to shelter senior al-Qaeda leaders and allow them to conspire with other terrorists.

We have witnessed their cyber attacks on our industry and local government. We thwarted their plots to conduct assassinations in the United States and we have arrested their operatives for surveilling critical infrastructure and plotting attacks on our homeland. We must remain vigilant in the face of these threats. It is more important than ever for Americans to report suspicious activity to law enforcement at every level to share information and intelligence on threats to our security.

Nearly all committee Members attended the threat briefing with senior DHS officials last week to learn more about the Iranian threat and the Department's response. I want to commend the Acting Secretary Wolf for the actions the Department is taking to mitigate the threat from Iran. I look forward to continuing this committee's bipartisan efforts to ensure DHS has the authority and resources it needs to successfully counter the threat from Iran and other sponsors of terror.

I thank the witnesses for coming and I thank each of them for their service to our Nation. I look forward to a constructive hearing and good discussion on what actions the Government should take to counter the threat from Iran, and I yield back.

[The statement of Ranking Member Rogers follows:]

STATEMENT OF RANKING MEMBER MIKE ROGERS

JANUARY 15, 2020

Iran has been escalating tensions in the Middle East for decades.

Since the nuclear deal was signed, Iran's malign activities have only increased.

The $100 billion in assets released by the Obama administration helped Iran enhance the manpower and capability of its terrorist proxies.

It helped Iran to conduct vicious cyber attacks on private industry and allied nations.

It enabled them to grow their missile stockpiles and improve their lethality.

Six months after it signed the JCPOA, Iran conducted ballistic missile tests with missiles carrying the inscription "Israel should be wiped off the earth."

It is clear the Obama-era policies of appeasement did not work.

The President was right to take the United States out of the JCPOA and reimpose sanctions on Iran.

The President understood that the JCPOA was not going to contain Iran.

That flawed deal was doing nothing to end the very clear and direct threat the Iranian regime poses to the United States, Israel, and the rest of our allies.

For over a decade, Iran has funneled money, terrorists, and advanced weapons to its proxies in Iraq, Syria, and Lebanon, who used them to attack U.S. troops and Israeli citizens.

In so doing, Iran is responsible for the deaths of over 600 Americans.

The latest American murdered at the hands of Iran was civilian contractor and father of 2 young children in California.

Fortunately, the President took decisive action to eliminate the brutal terrorist primarily responsible for his death and the deaths of thousands of others.

Qussem Souleimani was sanctioned as a terrorist by the United Nations and the Obama administration.

For over 20 years, he led the IRGC's Quds Force, a foreign terrorist organization.

Souleimani was not visiting Baghdad because it's a great holiday destination.

He wasn't there as some peace envoy.

He was there to meet with the leader of a terrorist group to plan more attacks on Americans.

The President used the law and his Constitutional authority as commander-in-chief to eliminate this terrorist mastermind before he could kill again.

For the first time in years, Iran received the message that there will be real consequences should they continue to threaten the United States and our allies.

I hope Iran understands this message and finally ends their malicious and destabilizing actions in the Middle East.

I also hope the Iranian regime understands that the United States will not hesitate to defend our homeland against any threat they advance.

For years, the Department of Homeland Security, the FBI, and other law enforcement partners have kept close watch on Iran's intentions and its capability to strike our homeland.

The threat from Iran is real.

We know they continue to shelter senior al-Qaeda leaders and allow them to conspire with other terrorists.

We've witnessed their cyber attacks on our industry and local government.

We've thwarted their plots to conduct assassinations in the United States.

We've arrested their operatives for surveilling critical infrastructure and plotting attacks on the homeland.

We must remain vigilant in the face of these threats.

It is more important than ever for Americans to report suspicious activity and for law enforcement at every level to share information and intelligence on threats to our security.

Nearly all committee members attended a threat briefing with senior DHS officials last week to learn more about the Iranian threat and the Department's response.

I want to commend Acting Secretary Wolf for the actions the Department is taking to mitigate the threat from Iran.

I look forward to continuing this committee's bipartisan efforts to ensure DHS has the authority and resources it needs to successfully counter the threat from Iran and other sponsors of terror.

I thank the witnesses for coming and I thank each of them for their service to our Nation.

I look forward to a constructive hearing and a good discussion on what actions the Government should take to counter the threat from Iran.

Chairman THOMPSON. Thank you very much. Other Members of the committee are reminded that under the committee rules opening statements may be submitted for the record.

I welcome our panel of witnesses today. Our first witness, Ambassador Barbara A. Leaf is the Ruth and Sid Lapidus fellow and director of the Geduld Program of Arab Politics at the Washington Institute for the Near East policy. Ambassador Leaf served as U.S. Ambassador to the United Arab Emirates from 2014 to 2018.

Next we are joined by Lieutenant General Vincent R. Stewart who served as a special advisor and chairman of Middle East Media Research Institute Board of Advisors. Lieutenant General Stewart formally served as the deputy commander of the U.S. cyber command and director of the Defense Intelligence Agency.

We also are joined by Mr. Thomas Warrick, a non-resident senior fellow at the Atlantic Council. Mr. Warrick previously served as the deputy assistant secretary for counter-terrorism policy at the Department of Homeland Security from 2008 to 2019.

Finally, we are joined by Brigadier General Anthony Tata, the CEO and president of Tata Leadership Group. After retiring from a 28-year career in the United States Army, Brigadier General Tata recently served as North Carolina's Secretary of Transportation.

Without objections the witnesses' full statement will be inserted in the record.

I now ask each witness to summarize his or her statement for 5 minutes beginning with Ambassador Leaf.

STATEMENT OF BARBARA A. LEAF, DIRECTOR, GEDULD PROGRAM ON ARAB POLITICS, WASHINGTON INSTITUTE

Ms. LEAF. Chairman Thompson, Ranking Member Rogers, distinguished Members of the committee, what comes next after the January 3 killing of Quds Force commander Qassem Soleimani and a senior Iraqi militia commander?

In my view we cannot take literally Foreign Minister Zarif's statement that with Iran's missile strikes on U.S. Forces in Iraq, Iran has concluded proportionate measures in self-defense. Rather, we are in a pause in an escalatory cycle. The factors driving this cycle are numerous, although Soleimani's quest to drive the United States from the region is long-standing.

The essential stalemate between Washington's maximum pressure campaign and Tehran's maximum resistance campaign: Tehran's view that it is already in a war, an economic war waged by the United States. Its leaders' conviction that they have staying power and tools that the United States lacks. Attacks on shipping, assassinations, terrorism, formidable regional proxies, providing Tehran myriad ways to continue countering U.S. pressure. Thus the impasse. Thus the continuing threats.

I will focus here on Iraq and the Persian Gulf where Tehran will almost certainly revert to a campaign of pressure. In Iraq, Tehran has long judged, enjoys a decisive advantage over the United States in influence and coercive tools. In the Gulf, Tehran has repeatedly demonstrated to Washington's closest allies their strategic role and abilities are acute, notwithstanding the presence of longstanding U.S. military facilities and thousands of U.S. service members.

In Iran, Soleimani leaves behind a well-oiled disciplined machine acting on behalf of a regionally powerful, if economically stressed, state. In Iraq, Iranian-affiliated militias are pushing hard to fulfill

his vision, forcing the departure of the 5,000 strong U.S. military training mission. The pressure is unrelenting within the government on Shia and Kurdish politicians and most brutally against Iraqi protestors who reject both Iranian interference and the recent threat-induced parliamentary vote.

The Iraq of 2020 aptly reflects Soleimani's efforts in Iraq, always weak vis-á-vis Iran and the government, itself, suborned and weakened by a set of proxy armed actors not under the state's control and largely pliant under Iranian direction. Today some 3 dozen such militias operate in Iraq commanding some 60,000 members.

They flout Iraqi law and the Constitution, operate training sites and arms depots that are no-go zones for the Iraqi security forces. They have repeatedly targeted U.S. military sites and U.S. diplomatic facilities over the past 18 months; participate in Iran's program to transfer advance missile technology to Lebanese Hezbollah and targeted the Saudi East West Pipeline.

Whether these militias will take on a future Hezbollah style role abroad, acting on Iran's behalf is as yet an open question. While fully half of the 70- to 80,000 U.S. forces deployed in the Middle East are ranged across the 6 GCC countries, these countries have felt extraordinarily exposed and vulnerable amidst escalating tensions between the United States and Iran, and Iranian attacks on Gulf energy infrastructure and oil tankers in 2019.

They are acutely vulnerable to Iran's full suite of asymmetrical tools, cyber in particular. A prolonged takedown of the electrical grids alone would be devastating. I will say that the administration's responses throughout that period of last year's attacks by Iran were contradictory and somewhat confusing.

This and the lack of U.S. response to the earlier attacks appear to have led Tehran to calculate that it bore little risk of reprisal, especially in September 2014. Why do these activities in the Gulf or in Iraq via proxies, matter for U.S. Homeland Security?

Number 1, oil. Notwithstanding the new U.S. role as an energy mega giant, oil remains a global commodity, its price affected directly by security or insecurity in the Persian Gulf, carrying a knock-on effect for economies including our own.

Number 2, counterterrorism. Our ability to pursue robust counter-terrorism efforts with dependable allies directly affects our security at home. Sustaining critical training for Iraqi security forces, intelligence sharing and acquisition leading the enduring defeat of ISIS in Iraq and Syria are now very much in question. ISIS cell attacks in Iraq alone last year numbered nearly 900.

If we are compelled to pull U.S. trainers from Iraq, sustaining them in Syria will be impossible in my view.

Finally, regional stability. In Karim Sadjadpour's words, Qassem Soleimani's sinister genius was marshalling both Sunni and Shia extremists to bring a wrecking ball earlier to the U.S. project in Iraq, then building out a foreign legion to expand Iran's influence far across the Arab Middle East.

This project of constructing parallel institutions to the state that suborn it and follow foreign direction is vividly on display in Iraq, Syria, and Lebanon. It's a recipe for chronic instability and insecurity across a widening arc of territory that is home to nearly 70 million people, the globe's fourth-largest oil producer, source of a

global extremist scourge and source of more than 8 million refugees.

Thank you.

[The prepared statement of Ms. Leaf follows:]

PREPARED STATEMENT OF BARBARA A. LEAF

JANUARY 15, 2020

Chairman Thompson, Ranking Member Rogers, distinguished Members of the committee, thank you for the opportunity to come before the committee today to discuss a set of issues which has gripped the U.S. Government, the Congress, and indeed, much of the American public for the last 2 weeks. The subject you have asked me and my fellow panelists to address is a critical one—the homeland security implications of rising U.S.-Iran tensions; specifically, what we might anticipate in the aftermath of the U.S. lethal targeting of Qassem Soleimani on January 3. I would like to acknowledge up front a debt I owe to the invaluable primary research and analysis on the Shia militias that form Qassem Soleimani's "foreign legion" of proxies, done by my colleagues at the Washington Institute, Phillip Smyth and Michael Knights, work which has been invaluable background for my discussion today.

Four days after Soleimani's death, Iran responded dramatically, with a volley of ballistic missiles directed at 2 bases hosting U.S. military trainers in Iraq. We cannot take FM Javad Zarif's statement immediately afterwards—that Iran has "concluded proportionate measures in self-defense"—as a signal that Tehran's missile strike definitively brings this matter to a close, however. Rather, we are in a pause in an escalatory cycle, one in which the United States and Iran are very likely to find themselves once again facing decisions on a kinetic response, sooner rather than later.

The factors driving this cycle are numerous, although Soleimani's vision to drive the United States from the region is long-standing—the essential stalemate between Washington's "maximum pressure campaign" and Tehran's "counter-pressure campaign" sets the more immediate context; Iran's move up the escalatory ladder was on vivid display last summer in the waters of the Persian Gulf, against Saudi Aramco, and in repeated attacks on U.S. military and civilian personnel in Iraq. Tehran's view is that it is already in a war, an economic war waged by the United States, but its leaders are equally convinced that they have staying power and tools that the United States lacks. Iran has developed doctrine, systems, and methods for operating in the "gray zone" rather than in head-on conventional conflicts, and its array of asymmetrical tools, which range from attacks on shipping, assassination, terrorism, to a formidable array of regional proxies provide it the way to continue countering U.S. pressure. While wreaking revenge. As Suzanne Maloney put it recently, "The regime's determination to end the American siege is magnified by an ideological and strategic zeal to settle scores for Soleimani's death, to preserve or even expand the footprint that he achieved for Iran across the broader Middle East, and ideally emerge from this crisis with some big strategic gain, such as durably eroding U.S. presence and influence in the broader Middle East."

I would like to focus in my remarks on the geo-political ramifications of Jan. 3, in particular in Iraq and the Persian Gulf, two arenas where Tehran is most likely to look for opportunities to avenge Soleimani's death. It is there that Tehran will almost certainly revert to a campaign of pressure and attacks. In Iraq, Tehran has long judged it enjoys a decisive advantage over the United States in influence and coercive tools. In the Gulf, Tehran has repeatedly demonstrated to Washington's closest allies that their strategic vulnerabilities are acute, notwithstanding the presence of long-established U.S. military facilities and thousands of U.S. service members.

If ever two adversaries of the United States brought on their own deaths, it was Iranian Quds Force Commander Qassem Soleimani and Jamal Jaafar Ibrahimi (AKA Abu Mahdi Al Muhandis), commander of the Iraqi militia Kata'ib Hezballah. Killed as they departed Baghdad airport together, Soleimani and Al Muhandis were long-time collaborators in a common project to target U.S. troops to drive them out of Iraq; their pioneering handiwork in the use of explosively-formed projectiles (EFP) killed hundreds of U.S. service members and maimed thousands more. More recently, KH's task from Soleimani—to harass and target U.S. military personnel with repeated shelling of training sites over much of 2019—finally resulted in the death of an American on Dec. 27; the U.S. response 2 days later, targeting 5 KH sites, was met with a violent assault by the militia and its supporters on the U.S. Embassy in Baghdad.

Both architect and orchestrator of Iran's destructive regional policies in Syria, Lebanon, Iraq, Yemen, and Bahrain, Soleimani had achieved a singular stature in Iran and in the wider Middle East by dint of his own extraordinary media profile and the multiple successes he claimed on behalf of Tehran: For turning the tide of Syria's civil war to Bashar Al Assad's favor; for being first on the battlefield in 2014 as ISIS forces surged across northern Iraq toward Erbil; for his small-investment-huge-payout decision to train and equip Yemen's Houthis with advanced missile technology, such that they could strike deep into Saudi territory, threaten the UAE and put international shipping in the Bab Al Madeb at risk; for his unmatched role as kingmaker or breaker in Iraq, in no small part through the network of militias he had created, groomed, trained, and resourced from the early months after the 2003 invasion of Iraq. As my colleague, Phillip Smyth, has neatly put it, "Iran's Shia militia network are their true nuclear program and one that has achieved measurably huge results for Tehran" in the region.

At the time of his death Soleimani thus appeared to be a Colossus bestride the region. He was a cult figure for Iran's legions of foreign Shia proxies, and an interlocutor respected and feared in equal measure by officials in Iran's near-beyond.

But if Soleimani's demise at U.S. hands has electrified both regional and foreign audiences, the operation's second major casualty—collateral damage or intended target, depending on the U.S. official asked—is potentially as impactful for Iraq, and therefore for U.S. interests. Al Muhandis was both head of the most powerful militia in Iraq, Kata'ib Hezballah, and as Deputy Commander of the PMF exerted far-reaching command and control over nearly 50 other organizations in the PMF network; his killing will have direct bearing on the future of the U.S. military presence in Iraq and our ability to counter terrorist threats to the U.S. homeland.

IRAQ

History shows us that removing a leader of violent movements—even one as supremely capable, influential, and charismatic as Soleimani—is rarely sufficient on its own to permanently disrupt the trajectory of events or even the organization itself. In Iran, Soleimani leaves behind a well-oiled, disciplined machine acting on behalf of a powerful, if economically stressed, state. Iran's Supreme Leader moved immediately to appoint Ismail Qaani, Soleimani's deputy in the Quds Force, as successor. This move reinforced the dual message of organizational continuity and Iran's relentless commitment to the Resistance cause. In the days to follow, IRGC leaders underlined the latter point in public messaging: With the commander of the IRGC flanked by the flags of member groups of regional resistance, including that of Iraq's Hashd al Shaabi, and with IRGC-Quds Force commander Qaani's meeting with individual commanders of Iraq's Shia militia community.

In Iraq, a hard push by Iranian-affiliated militias—through their representation at the highest levels of the Iraqi government and their political representation in the parliament—has resumed to affect the departure of the 5,000-strong U.S. military training mission. Qassem Soleimani's project for post-ISIS Iraq was to end the U.S. military presence in Iraq, and with its departure, to reduce to the degree possible U.S. influence there. An earlier effort in Iraq's Council of Representatives in the spring of 2019 was sidelined. But in the wake of Soleimani's death, the Council passed a non-binding resolution requesting the government begin the process for ending the foreign troop presence in Iraq; passed with a fraudulent quorum, the vote was obtained after overt threats by KH and its allies against MPs. Notwithstanding those threats, virtually all Kurdish and Sunni MPs stayed away from the vote. And notwithstanding the fraudulent nature of the parliamentary vote, Iraq's acting PM repeatedly announced his request of the United States to begin consultations on winding up the U.S. military mission.

The pressure by Iranian-backed militias is unrelenting—within the government, on the acting PM, on Shia and Kurdish politicians, and most brutally, against the throngs of Iraqi protestors across Baghdad and southern, Shia-dominated Iraq, who have rejected both Iranian interference and the recent threat-induced parliamentary vote.

Prominent Iraqi militia leaders like Asaiab Ahl Al Haq's Qais al Khazali have publicly declared that Tehran's missile strike, while honoring Soleimani, would not suffice as a response for Al Muhandis' death. Iraqi militia leaders have made overt threats to resume kinetic targeting of U.S. military personnel; indeed, there have been several instances of rockets falling in Baghdad since the Iranian missile strikes. For the moment, Iraq's Iranian-affiliated militia community appears to be following Tehran's direction to pause, but that is a pause likely to be short-lived.

THE PMF PROBLEM

Iraq's evolution since 2003 has been as much shaped by Qassem Soleimani's vision for the country as by the energy, money, and lives spent under 3 successive U.S. administrations. Soleimani's focus on Iraq was unblinking and unsparing; his approach reflected the perspective of a war-time generation of leaders, that Iraq posed the foremost National security threat to Iran. Thus Soleimani worked methodically and largely successfully for a set of unvarying objectives there: An Iraq always weak vis-á-vis Iran, its Shia-majority political class reliant on and deferential to his "guidance," and above all, the government itself suborned and weakened by a set of proxy armed actors not under the State's control and largely responsive to Iranian direction. Today approximately 3 dozen such militias operate in Iraq, commanding some 60,000 members.

The Iraq of 2020 aptly reflects Soleimani's efforts. With the departure of U.S. troops in 2011, Iraqi militias were re-directed by Soleimani to Syria's civil war, where they gained critical battlefield experience, under IRGC–QF direction fighting on behalf of Bashar Al Assad. In the crisis of ISIS' surge across northern Iraq in 2014 and with Grand Ayatollah Sistani's exhortation to Iraqi youth to volunteer for the fight, Soleimani oversaw and shaped directly the explosion of Iraqi militias and took a role on the battlefield in directing their efforts. In 2016 the militias were folded formally into the Iraqi security forces and termed the Popular Moblilization Forces. Iraqi National Security Advisor Falah Fayyad is double-hatted as its commander, but the real power to the organization lay with its Deputy, KH Commander Abu Mahdi Al Muhandis—not with the PM, to whom, Commander-in-Chief, the PMF notionally reported. Securing the funding of the state, the member militias of the PMF from the outset retained a dual-key chain of command, retaining primary loyalty to their political commanders, many of whom in turn followed Iranian "guidance," if not direction.

These militias flout Iraqi law and the constitution in myriad ways; they did so in recruiting fighters for Syria, and they do so currently in operating training sites and arms depots that are no-go zones for the Iraqi security forces. But nowhere has that allegiance to a set of leaders outside the State—outside Iraq itself—been more evident than in the repeated targeting of U.S. military training sites and U.S. diplomatic facilities by KH, AAH and other militias for the past 18 months; their participation in Iran's program to transfer advanced missile technology to Lebanese Hezballah; and KH's targeting of the Saudi East-West pipeline.

Thus is born a militia state, or one at real risk of becoming so. With the fall of Mosul to Iraqi government forces in December 2017, the Iraqi government should have moved to complete the transformation or compulsory demobilization of the constituent members of the PMF into the ISF. It was unable to do so. As recently as September 2019 the Iraqi PM felt compelled to issue an ultimatum to the PMF to hand over weaponry to the state, permit ISF access to militia arms depots and bases, and to cease all unlicensed activities. The reason? Press reports identifying KH as the entity behind the May 2019 attack on Saudi Arabia, and months of apparent foreign airstrikes on KH arms depots that were supporting Iran's work to transfer advanced missile technology to Lebanon for Hezballah. But to no effect.

With Abu Mahdi Al Muhandis's death, and a successor still unnamed, the key Iraqi militias of significance, closest to Iran, remain in a state of uncertainty. They are maneuvering rapidly to try to shape the next government, however.

The most important of the militias closely affiliated with the Quds Force—the Badr Organization, Kata'ib Hezballah, Asaib Ahl Al Haq, Kata'ib Al Imam Ali, Kata'ib Sayyid Al Shuhada—also command the lion's share of the PMF rank and file, 18–25,000 for Badr alone, and the rest comprising somewhere in the range of 31,000 members. They have all deployed "in-theatre"—in Syria; several participate actively in Iran's "precision missile" project to move parts and technology from Iran through Iraq and Syria to Lebanon; several have engaged in lethal support and training for extremists in Bahrain, and 1—KH—to date has engaged in attacks outside Iraq/Syria, on Saudi Arabia. While smaller by far in numbers, the phenomenon of drawing foreign fighters into their ranks from Europe (generally dual-national citizens) to fight in militia ranks in Syria has been observed. One possible model for the future—the risk of reverse flows, establishment of cells abroad as Hezballah has done successfully—should certainly not be ruled out.

THE GULF

The long-standing U.S. military presence in the Middle East ranges currently between 50–65,000 personnel, fully half of whom at any given time may be stationed in the 6 Gulf Cooperation countries. While the U.S. naval presence in Bahrain, now headquarters of the Fifth Fleet, dates back to the late 1940's, our operating presence

in the other Gulf countries largely date to immediately after the first Gulf War; U.S. forces in Saudi Arabia being a particularly sensitive issue internally, the United States has not had "permanent" stationing of troops there since 2003, although the administration has sent several thousand to the Kingdom in recent months in response to last year's attacks on Saudi energy infrastructure by Iran.

Yet despite that presence, there is no question that the GCC countries—with the possible exception of Oman—have felt extraordinarily exposed and vulnerable for the last 8 months, a period of sustained, escalating tensions between the United States and Iran and thinly-disguised attacks by the latter on Gulf energy infrastructure and oil tankers traversing the Gulf. Persian Gulf energy fuels the world economy, meeting nearly 20 percent of global demand. But these small and vulnerable states are also uniformly embarked on efforts to diversify their economies away from fossil fuel dependency, redefining themselves as hubs for tourism, transportation, finance and banking, and manufacturing—sectors which depend every bit as global oil markets do on a secure and stable environment.

Notwithstanding decades-long huge investments by the GCC countries in U.S. and European weapons systems, including missile defense, these 6 countries remain hugely vulnerable. With small populations, economies which have developed with a significant dependency on expatriate labor, the GCC countries are particularly vulnerable to Iran's full suite of asymmetrical tools, cyber in particular. For countries that rely on desalinization for 95 percent of their potable water supply, that import 90–95 percent of their foodstuffs, that have diversified their economies by making themselves hubs for global trade, air traffic, shipping and finance, a prolonged takedown of the electrical grid alone would be devastating.

U.S.-Iran tensions soared with the administration's announcement in April 2019 that it would aim to "drive to zero" Iran's oil exports; a stark U.S. warning to Iran followed on May 5—asserting intelligence indicated possible Iranian intentions to target American citizens or facilities in the Gulf and Iraq—that any Iranian attack on "U.S. interests or those of its partners (would) be met with unrelenting force." Iran responded exactly 1 week later with attacks on 4 tankers berthed off the UAE coastline; 2 days later, the Saudi East-West pipeline was hit by explosive-bearing drones, later determined to have been launched by one of Iran's closest proxies in Iraq, Kata'ib Hezballah. Thus ensued months of thinly-veiled attacks by Iran—on a U.S. drone, on Saudi oil pipelines, on foreign tankers, and most spectacularly on Sept 14, on the heart of the Saudi energy enterprise in Abqaiq.

The administration's responses throughout these months were contradictory and confusing. Secretary Pompeo made an early trip to Baghdad to warn Iraqi leaders—who we can be certain passed this message immediately to Tehran—that the United States would respond immediately, forcefully to any move against an American citizen. But this warning—and U.S. non-response to the series of Iranian attacks against Gulf partners, international shipping, even to the downing of a U.S. drone—had the ironic effect of so strictly de-limiting what would be "off limits" that it appears Tehran boldly calculated it could land a strategic strike on Saudi Arabia and bear little risk of reprisal. This calculation was borne out, in fact.

In the aftermath of Soleimani's death and Iran's for-now limited response, the question for Washington's Gulf partners remains unanswered—does the U.S. security umbrella extend to them? If Iran returns to attacks on shipping or energy infrastructure, will the United States respond—and if so, how? If Saudi Arabia suffers a further, more devastating attack, what then?

CONCLUSION

Americans are pressed by the events of the last 2 weeks to ask: Why do Iran's activities in the Gulf or in Iraq, via proxies or directly, matter for U.S. homeland security?

No. 1: Oil: notwithstanding the new U.S. role as an energy mega-producer, oil remains a global commodity, its price affected directly by security—or insecurity—in the Persian Gulf, carrying a knock-on effect on global economic health, including our own. The administration appears uncertain about how much longer the United States should wear the mantle of ensuring the free and unconstrained flow of energy and commerce in the Persian Gulf. Iran picked up on that ambivalence, as did our Gulf partners.

No. 2: Counter-terrorism: Our ability to pursue robust counter-terrorism efforts in concert with dependable allies goes directly to our security at home. Whether we will be able to sustain a critical capability-building mission for Iraqi security forces, benefit in intelligence-sharing and gathering from being there on the ground, and help direct efforts to drive toward an enduring defeat of ISIS in Iraq and Syria are now very much in question. ISIS cell attacks in Iraq alone numbered nearly 900

in 2019. And if we are compelled—or choose—to pull U.S. trainers from Iraq, sustaining them in Syria is likely to be impossible. In the same vein, the relations of trust and confidence and influence that we sustain with our Gulf partners are critical to CT efforts by/through/with their policy makers, intelligence, defense, and finance officials.

No. 3: Regional stability: Karim Sadjapour aptly noted this week Qassem Soleimani's "sinister genius" in marshalling both Sunni and Shia extremists to bring a wrecking ball early on to the U.S. project in Iraq, then building out "a foreign legion" to expand Iran's influence far across the Arab Middle East. Soleimani's terrible legacy—constructing parallel institutions to the state that suborn and overpower it, and follow foreign direction—is vividly on display in Iraq. It is a recipe for chronic instability and insecurity across a widening arc of territory that is home to nearly 70 million people; home to the globe's fourth-largest oil producer, source of a global extremist scourge, source of more than 8 million refugees.

What should the United States do? Navigating the turbulence besetting Iraq will be paramount, to ensure the critical U.S.-led Coalition counter-terrorism mission there can endure, and U.S. military trainers can operate safely. That will require more vigorous and more visible engagement from Washington, backstopping the tough work in which our Ambassador and diplomatic staff in Baghdad and Erbil are engaged. And to be most effective, that effort should be robustly multilateral, drawing on the Coalition and the United Nations. Much has been made this past week on the administration's support for Iran's protestors, but shockingly little attention has been spared for Iraqis who have suffered and died for more than 3 months to press many of the same demands. Washington should unequivocally signal support for the protestors across Iraq seeking a new government, via early, clean elections; those same protestors have been the victims of Soleimani's militia project, targeted for assassination and brutal repression in the streets. Washington should focus its pressure, with targeted sanctions on both the senior government officials and the militia commanders responsible for the repression.

While the administration has asserted that "deterrence has been restored" with Soleimani's death, it is fair to ask when it was lost. And deterrence, to be enduring and effective, cannot be built on a single action, however dramatic. The U.S. security umbrella for the Persian Gulf is well-tattered, and an honest discussion between the United States and its partners on how to restore it—including what that requires of our quarreling partners—is long overdue.

Finally, it goes without saying that the time for vigorous diplomatic work is also upon us, lest the United States and Iran simply return to what I think of as a 40-year-long frequently violent non-relationship. The asymmetrical threats to U.S. interests and security, to those of our friends in the region, that Qassem Soleimani constructed in more than 2 decades of dedicated work will not be undone through economic sanctions alone, nor do they lend themselves for the most part to a military response.

As Ariane Tabatabai wrote in 2019, "One thing the Iranians do not lack is options. The regime can use the (threat network) as a strike force to further its foreign policy goals in the region." The United States, too, has a range of options to contend with any of the threats to homeland security—indirect or otherwise—that Iran considers over the months ahead. One of the most important options for the administration to exercise now is diplomacy, even as we keep economic, cyber, covert, and conventional military tools at the ready to contain, deter, and disrupt Iranian resort to asymmetrical warfare. As the dust settles on the 2 matching "black swan" events of the last 2 weeks—the most consequential U.S. strike on a foreign government official in modern times, and the first conventional Iranian attack on U.S. forces since the Iran-Iraq war—it is time to turn swiftly to identify the channel and the pathway to negotiations.

Chairman THOMPSON. Thank you for your testimony.

I now recognize Lieutenant General Stewart to summarize his statement for 5 minutes.

STATEMENT OF VINCENT STEWART, SPECIAL ADVISOR AND CHAIRMAN, BOARD OF ADVISORS, MIDDLE EAST MEDIA RESEARCH INSTITUTE

General STEWART. Good morning, Chairman Thompson, Ranking Rogers, and other distinguished Members of the committee.

I'm honored to be here as an advisor to the Middle East Media Research Institute, an organization for the last 20 years that

looked at the social and intellectual currents within Iran. I'd like to step back just a little bit as we talk about this situation in Iran as this continues to unfold.

I believe it is more important than ever that we pause and put whatever short-term actions Iran takes into longer-term context, via 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 themself.

With that I'd like to start with Iran's theory of victory or their desired end-state. Iran believes that it is the dominant regional and cultural power, and the United States and its allies in the region are impediments to Iran's desired end-state. The Iranian government believes they are the victim of U.S. actions, are, in fact, rational actors protecting the region and themselves from undue foreign influence.

Iran believes it will successfully force the United States to leave the region. But the question is since we are obviously stronger conventionally, how does Iran believe it can accomplish its end-state? Iran understands that its military capabilities will not deter the United States from conducting military actions and that they would eventually be overmatched by our armed forces.

Iran has built a capable force of an imposed cost on the United States, its allies, its forward staging basis and its interest in the region, but cannot militarily match U.S. capabilities in the long term. However, Iran views asymmetric activities as a viable cost means—low-cost means to eject the United States from the region. Iran's asymmetric warfare can be viewed as a three-legged stool comprising of 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 United States and avoiding the threshold of an overt U.S. military response. Since Iranian military support to terrorists and malign actors is covered in the extensively and classified reporting, I'll focus on the second and third legs of the stool.

Iranian information operations, influence operations are not well-understood and target several audiences, but most important is their own domestic population, which the regime seeks to keep united around nationalism and a perceived victimhood. Like-minded terrorists, militants, and religious groups are also key constituencies.

Iran's fastest-growing audience are international, Russia and China, and increasingly U.S. allies in the region and abroad. Last, I want to highlight that with the rise of social media and the ease of transmitting messages, the Iranians increasingly see different factions inside the United States as information operation 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.

So what are some of the messages from the Iranians? Geography matters. Iran has no options of leaving the region. We have a population of 80 million people. They have a rich history of culture and heritage and we will be here when the Americans leave. In spite

of the propaganda, what they perceive as U.S. propaganda that they are destabilizing the region, that they are, in fact, rational actors on the international stage and conform to international norms of behavior. They go through this litany. "We have complied with the joint comprehensive plan of action. We have taken the responsible action to defend our country after the attack on Soleimani", and so they continue to emphasize those messages.

The bottom line on Iranian information operations is this: Anything that gives the regime narrative a boost is a victory on the path to Iran's theater victory. Their three-legged stool of asymmetric warfare is carefully calibrated.

The cost of U.S. presence is high while cultivating an image of being rational actors and victims. All actions and the reactions must be viewed through those lens. The third leg of their asymmetric warfare is cyber space and we will spend a good bit of time talking about that during this hearing. Since the Stuxnet event, Iran has embarked upon a comprehensive approach; developed both offensive and defensive cyber capabilities. We have seen them exercise those capabilities against nation-states, Saudi Aramco, against small companies, against our own financial system, and the Sands Casino in 2017.

In the interest of time, the Iranians are not as capable as the Russians or 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 interests. They have demonstrated an ability to conduct attacks, incurring costs to private U.S. companies, foreign entities in the multi-billion—million-dollar ranges. They will include cyber space operations as a key component of their asymmetric response to the killing of Soleimani. What makes this foreign threat so unique is that this is the one area where the U.S. Government is essentially telling the U.S. private sectors to fend for yourself. I'll stop there and I look forward to your questions.

[The prepared statement of General Stewart follows:]

PREPARED STATEMENT OF VINCENT STEWART

"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 U.S. actions and are in fact

the rational actor protecting the region and themselves from undue foreign influence. Iran believes it will successfully force the United States 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 United States 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 United States' 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 United States 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. Last, I want to highlight that with rise of social media and ease of transmitting messages, the Iranians increasingly see different factions inside the United States 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 3,000+ year history, culture, and heritage—we will be here when the Americans leave.
- In spite of U.S. 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 United States 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 toward 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 cyber space. Iran views cyber space 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 9 Iranians in a wide-scale cyber-theft campaign, stealing more than 31 terabytes of documents and data from more than 140 American universities and 30 American companies. Previously in March 2016, the United States charged 7 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 World-wide Threat Assessment of January 2019 said that Iran was attempting to build cyber capabilities that would enable attacks against critical infrastructure in the United States and elsewhere. It stated that "Iran has been preparing for cyber attacks 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 cyber attacks 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

---

[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.

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]

ROUND-UP OF RECENT CYBER INCIDENTS WITH IRANIAN INVOLVEMENT [10]

- *January 6, 2020*.—The website of the Texas Department of Agriculture was hacked and its home page 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 cyber espionage 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 United States, Australia, United Kingdom, 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 United States, 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 cyber attacks. 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 on-line, 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 cell phones, in industrial equipment and . . . neutralize them.

"Dejfa is used to discover damage done by malware on-line, such as bots, identifying the type of malware by anti-virus collection and neutralization. [Using Dejfa]

---

[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.

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 cyber space, 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 cyber attack on Iran: "An organized cyber attack 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 cyber space . . . "[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 cyber space 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]

---

[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.

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 cyber attack 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 cybersecurity 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 cybersecurity. The solution for cybersecurity 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 4 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 cyber space.

"We have 5 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 cybersecurity experts in the next 4 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.

---

[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.

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 cyber space.[29]

July 15, 2019.—Basij lieutenant commander Mohammad Hossein Sepehr said at the closing ceremony for the eighth assembly for cyber space admins: "Khamenei says that 'cyber space is as important as the Islamic revolution.' The cultural field is part of jihad. If we leave cyber space we will probably be hit. At this time, the Western faction is the most arrogant in its power in cyber space, due to its wealth, equipment, and other possibilities. At this time, the most powerful research is in cyber space . . . Some view cyber space 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 cyber space will be under the rule of Shi'ite followers of the 12 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 cyber space . . . "[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 toward 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

---

[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.

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 cyber war 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 Cyber Space, 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 cyber attack (such as Stuxnet or the Russian actions in the Ukraine) are still beyond Iranian capabilities." However, poorly-defended targets in the United States, 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 cyber attack 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 cyber attacks 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 cyber space 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 2 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 cyber space looks like. We need increased emphasis on public-private partnership to achieve "collective defense", and we need

---

[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.

increased emphasis on educating the populace on the real threat from cyber space activities.

I look forward to your questions.

Chairman THOMPSON. Thank you for your testimony.

I now recognize Mr. Warrick to summarize his statement for 5 minutes.

STATEMENT OF THOMAS S. WARRICK, NONRS. ESIDENT SENIOR FELLOW, ATLANTIC COUNCIL

Mr. WARRICK. Mr. Chairman, Ranking Member Rogers, Members of the committee, thank you for the opportunity to testify.

One week ago today, the IRGC fired 22 missiles at 2 Iraqi airbases. According to the *New York Times,* if the attack had killed Americans the options put in front of the President would have included cyber attacks to disable Iran's oil and gas sector. It is important this committee asks whether the United States oil and gas industry would have been ready for the Iranian cyber attack that would have followed.

Here is another question, not hypothetical. While Americans celebrated Thanksgiving, someone hit Iran with a massive cyber attack publicly disclosing 15 million Iranian debit card numbers on a social media site. The Iranians made the rare concession that this was, "very big". It is important this committee asks if our bank and credit card companies are ready if Iran tries to hack the card numbers of millions of Americans.

In my testimony I'm going to discuss the 4 ways Iran threatens the homeland. I want to make 3 preliminary points about Iranian cyber attacks and then focus on Iran's peculiar sense of symmetry as a means of understanding how they would carry out threats.

Mr. Chairman, Iran's 4 possible attack vectors are terrorism, cyber attacks, disinformation, and influence operations. Of these, terrorism is the least likely in the short term but it is still possible. The last state-sponsored attempted terrorist attack on U.S. soil was in 2011 when a group of IRGC Quds Force officers tried to assassinate the Saudi Ambassador in Washington, DC. Iran can also call on proxy groups like Lebanese Hezbollah.

No. 2, cyber threats, I'll come back to in a second.

No. 3, disinformation operations. Iran spreads false propaganda about the United States including the false idea that the United States actually supported ISIS, which obviously was not true.

Fourth, influence operations. As General Stewart said and as there was an outstanding exposé in *Wired* magazine in August 2018, I note more recently Facebook and Twitter have since found thousands of accounts linked to the Iranian government. Iran is getting better at influence ops.

Let me go back to cybersecurity and make 3 preliminary points. First, Iran and its allies considered the United States, Israel, and Saudi Arabia as responsible for each others' attacks. To be sure, we hold Iran responsible for the actions of its proxies.

Second, the Trump administration uses sanctions and cyber attacks as their go-to tools. U.S. officials have admitted twice on background to recent cyber attacks on Iran, and as I mentioned earlier, the option of a cyber attack after an American had been killed on January 8.

Third, the implication that it is safe for the United States to carry out cyber attacks against Iran is actually dangerous. Iran will retaliate but the cyber defenses of Iran's likely targets are uneven.

Mr. Chairman, this leads me to the most important point I would like you to take away from my testimony. Iran's government follows a peculiar sense of symmetry. When the United States does something to Iran, Iran tends to respond, not in exactly the same way but the symmetry is there. Some examples: After the January 2 strike against Soleimani, the Iranian Supreme Leader told his national security council to "strike America directly and in exact proportion to the attack".

More strategically, in May 2018, United States maximum pressure sanctions slashed Iran's oil exports. Iran tried to show that if the United States could cut Iran's oil exports, Iran could cut our allies' exports, in May and June with attacks on tankers and a Saudi pipeline, then with a September 14 Abqaiq attack that briefly cut Saudi oil exports in half.

Another symmetry: On July 4, Britain seized an Iranian tanker that was violating international sanctions. On July 19, Iran seized a British tanker. On August 15, the British authorities released the Iranian tanker. On September 27, Iran released the British tanker. There is symmetry in cyber space. After Stuxnet targeted Iran's industrial control systems in 2010, Iran developed a similar offensive capability and used it here in the United States in 2013. That took 3 years.

In August 2012, Iran's Shamoon malware deleted 35,000 hard drives at Saudi Aramco. What got less publicity is that 6 months earlier something called Wiper deleted data on national Iranian oil company computers. In July 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. The symmetry goes in the other direction.

When the Iran Nuclear Deal was enforced, Iranian cyber attacks appeared to drop. More recently after the 2018 maximum pressure campaign, Iranian cyber attacks increased. Within 24 hours after the June cyber attacks against Iran, private U.S. businesses noted an increase in Iranian cyber attacks.

Mr. Chairman, let me briefly mention 3 points about what the United States should do to defend the homeland.

First, any time the U.S. Government thinks about cyber offense it needs to focus just as much on cyber defense. Over time, Iran has improved its cyber capabilities, reduced its response time and shown it is capable of strategic surprise. This is especially a problem with Iran because of their peculiar sense of symmetry. Anything we do to Iran, Iran is likely to do back at us.

Second, while most Federal Government computers are protected, U.S. civilian cyber defenses are uneven. DHS and the FBI both need more resources to work more closely with the private sector.

Third, it is very good that DHS has increased its efforts since January 3 by repeating earlier warnings, issuing new alerts, putting out a new in-task bulletin and jointly releasing a joint-intelligence bulletin with the FBI.

The Trump administration needs now to increase and elevate its efforts to educate the American people about what they and we need to do to protect ourselves. Iran is going to be a threat for the foreseeable future. I'd be happy to answer any questions.

[The prepared statement of Mr. Warrick follows:]

PREPARED STATEMENT OF THOMAS S. WARRICK

JANUARY 15, 2020

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 2 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 cyber attacks "to partly disable Iran's oil and gas sector."

Would the United States oil and gas industry have been ready for an Iranian cyber attack 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 cyber attack: 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 cyber space 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 4 ways that Iran threatens the homeland. I would like to draw the committee's attention to 3 preliminary points about cyber attacks 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 cyber space.

FOUR WAYS IRAN THREATENS THE UNITED STATES

There are 4 possible attack vectors that Iran could use to target the United States: Terrorism, cyber attacks, 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 Jan-

uary 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 on-going.—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 CYBER ATTACKS

Mr. Chairman, permit me to go back to cyber attacks.

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 cyber attacks 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 cyber attacks 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 cyber space. 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 cyber space. In 2013, Iran developed a cyber attack capability after the "Stuxnet" malware that targeted Iran's Sie-

mens industrial control systems (ICS) came to light in June 2010. From Stuxnet's discovery until Iran's first ICS attack was 3 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 cyber attacks 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 cyber attacks increased within 24 hours.

On June 20, 2019, after Iranian attacks on civilian tankers, President Trump retaliated by cyber attack. Private U.S. businesses noticed a further increase in Iranian cyber attacks.

This leads to 3 important points: Over time, Iran has both improved its cyber capabilities and reduced its response time. What took Iran 3 years to respond to in 2010, and 6 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 cyber space, 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 U.S. POLICY MAKERS 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. policy makers consider kinetic strikes, they activate plans to notify and protect military and civilian personnel and facilities. The same logic should apply for cyber attacks, 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 cyber attacks 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 cyber attacks against Iran are necessary and why Americans should increase their cyber defenses, roughly analogous to the 1950's "civil defense" campaign.

However, drawing attention to the risks of cyber attacks 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 life-long 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 10 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.**

Chairman THOMPSON. Thank you very much for your testimony.

I now recognize Brigadier General Tata to summarize your statement for 5 minutes, and I hope I didn't ambush your name too much.

STATEMENT OF ANTHONY J. TATA, CEO AND PRESIDENT, TATA LEADERSHIP GROUP

General TATA. Chairman Thompson, Ranking Member Rogers, Members of the committee, thank you for inviting me here today for the privilege of providing comment on the important topics of homeland and National security.

Killing Qassem Soleimani and Abu Mahdi al Muhandis, both specially-designated terrorists, provides for a safer Middle East and a safer homeland in America. In strategy and in warfare, leadership networks and resourcing matter. Soleimani and Muhandis were experienced commanders overseeing a vast terror network that executed Iran's revolutionary strategy of exporting terror backed by Iran's $26 billion military budget.

Together they carried out 3 decades of terror against the United States and our vital interests and allies in the Middle East to include, but certainly not limited to, training, resourcing, and resupplying Shia militias in Iraq to disrupt U.S. operations, resourcing Hezbollah to attack Israel, planning and resourcing the thwarted attack on a Washington, DC restaurant a few miles from here, creating money-laundering schemes within the United States to fund

*Attachment has been retained in committee files.

terrorism, protecting the bin Laden family, al-Qaeda leadership and Taliban members immediately after the 9/11 attacks, training, resourcing and transporting Abu Musab al Zarqawi and other al-Qaeda members to fight coalition forces in Iraq, resourcing the Houthi rebels in Yemen to attack Yemen and Saudi Arabia, and resourcing and commanding multiple recent attacks against U.S. interests in the region.

Just as Osama bin Laden orchestrated the attacks that killed nearly 3,000 Americans, Soleimani orchestrated attacks that killed and maimed over 6,500 Americans through improvised explosive devices alone. Just as bin Laden continued to pose a clear and present danger to American interests world-wide until his death, so did Soleimani. Soleimani, however, was more dangerous than bin Laden because he was flush with resources from Iran, a designated state sponsor of terror whose defense budget has risen 60 percent between 2015 and 2018, from $16 billion to $26 billion.

Soleimani developed, refined, and deployed explosively foreign penetrators, lethal roadside bombs made of Iranian milled 6-inch copper discs, PVC or steel pipe, urea nitrate, a blasting cap, and typically a passive infrared switch trigger. When a target crossed the beam on the passive infrared switch, it ignited the blasting cap which, in turn, detonated the explosives, propelling a molten copper disc at 8,000 feet per second through its mark, killing and maiming whoever might be in the projectile's path of destruction.

Frequently, the destruction from an EFP sealed the vehicle's doors shut, leaving American soldiers to burn alive. Often Soleimani's EFPs were deployed in multiple arrays where several copper discs would punch through Humvees and other fighting vehicles, ripping arms and legs from service men and women. Soleimani and his chief lieutenant, Muhandis, were the masterminds behind and suppliers of these EFPs. Just in the last 18 months, 2 U.S. Federal judges each separately found Iran liable for their role in killing and injuring Americans in Iraq by providing material support to Iran's proxy terrorist groups.

Those U.S. District Court cases are *Karcher* v. *the Islamic Republic of Iran* and *Fritz* v. *the Islamic Republic of Iran,* which I have included in my testimony. Evidence in both cases proved that Soleimani and Muhandis, both senior leaders in Iran's IRGC Quds Force, acted on behalf of Iran to ensure Americans would die. Just one quote from witness testimony in those cases, from General David Petraeus, the MNF–I press conference he spoke at in April 2007 said, "And there's no question, again, that Iranian financing is taking place through the Quds Force of the Iranian Republican Guards Corps to support opposition forces in Iraq."

As they were moving freely about the region coordinating terror with Hezbollah and Shia militias in Iraq, Soleimani and Muhandis presented themselves in a designated combat zone as the leaders of a designated terrorist organizations, the Quds Force and Kata'ib Hezbollah. President Trump responded appropriately under the same authorization of use of military force that President Obama used against state and non-state actors in Iraq, Syria, Afghanistan, Yemen, the northern tier of Africa, and other locations.

While serving as the deputy commanding general of U.S. forces in Afghanistan in 2006 and -7, I directed several combat missions

to include drone strikes, artillery strikes, air assaults, and other operations, some of which found me on the ground with the soldiers conducting those missions.

Everything I've seen, read, and understand regarding the strike underscores its legality, importance, and proportionate nature to reset the balance of power in the Middle East with respect to U.S. interests and Iranian influence. The Soleimani strike is consistent with U.S. National security strategy as it relates to Homeland Security.

I brought a copy of the strategy today that the President published in 2017, that mentions pursuing threats to their source and defeating jihadist terrorists, and dismantling transnational criminal organizations, both of which the Quds Force is.

Practically, in my roles as an education leader here in Washington, DC and in North Carolina as secretary of transportation, and now as a chief executive with Air Data Solutions, I have been steeped in analysis of threats and responsibility for specific homeland security infrastructure and citizens over the last 10 years. To include—I am concerned about, including cyber attacks on key infrastructure such as airport, air traffic systems, physical security of soft target such as schools and mass transit for shock value, attacks on seaports to impact commerce, smuggling weapons and other resources to enable attacks, and biological warfare against crops affecting our food supply.

Finally, with Soleimani and Muhandis removed from the equation, we have an opportunity to positively reshape the dynamic in the Middle East toward peace and enhance homeland security. As a young United States Military Academy cadet, in 1981 my classmates and I witnessed first-hand the return of U.S. hostages in Iran to American soil at West Point, where they spent their first weeks reintegrating. The cruelty of the Iranian Islamic Revolution is seared in my memory and I'm personally proud that we have begun to fight back.

Thank you, sir.

[The prepared statement of Mr. Tata follows:]

PREPARED STATEMENT OF ANTHONY J. TATA

JANUARY 15, 2020

Chairman Thompson, Ranking Member Rogers, Members of the committee—thank you for inviting me here today to provide comment on the important topics of homeland and National security.

Killing Qassem Soleimani and Abu Mahdi al Muhandis, both Specially Designated Terrorists, provides for a safer Middle East and a safer homeland in America.

SOLEIMANI'S LEGACY OF TERROR

In strategy and warfare, leadership, networks, and resourcing matter. Soleimani and Muhandis were experienced commanders overseeing a vast terror network. Backed by Iran's $26 billion military budget,[1] together they carried out 3 decades of terror against the United States and its vital interests and allies in the Middle East, to include (but are not limited to):[2]

i. Training, resourcing, and resupplying Shi'a militias in Iraq to disrupt U.S. operations;

[1] Decoding Iran's Defence Spending, *International Institute for Strategic Studies,* November 13, 2018.

[2] *The Exile—The Stunning Story of Osama bin Laden and Al Qaeda in Flight,* Cathy Scott-Clark and Adrian Levy, Bloomsbury (2017).

ii. Resourcing Hezbollah to attack Israel;
iii. Planning and resourcing the thwarted attack on a Washington, DC restaurant;[3]
iv. Creating money-laundering schemes within the United States to fund terrorism;[4]
v. Protecting the bin Laden family, al-Qaeda leadership, and Taliban members immediately after the 9–11 attacks;
vi. Training, resourcing, and transporting Abu Musab al Zarqawi and other al-Qaeda members to fight coalition forces in Iraq;
vii. Resourcing the Houthi rebels in Yemen to attack Yemen and Saudi Arabia;
viii. Resourcing and commanding multiple recent attacks against U.S. interests:
- Shooting down 2 drones
- Seizing oil tankers
- Attacking Saudi oil fields
- Killing an interpreter and wounding 2 soldiers in Kirkuk
- Attacking the U.S. embassy in Baghdad.

Just as Osama bin Laden orchestrated the attacks that killed nearly 3,000 Americans, Soleimani orchestrated attacks that killed and maimed over 6,500 Americans through improvised explosive devices alone. Just as bin Laden continued to pose a clear and present danger to American interests world-wide until his death, so did Soleimani. Soleimani, however, was more dangerous than bin Laden because he was flush with resources from Iran, a designated state sponsor of terror, whose defense budget has risen over 60 percent between 2015 and 2018 from $16 billion to $26 billion.

Unlike bin Laden, who spent his final years as an isolated hermit, Soleimani was able to use his title and rank as a shield from prosecution and retribution. He skillfully used the Iranian-state apparatus as his "keys to the kingdom" of the Middle East. With approval from the highest-authority in Iran, the Supreme Leader, Soleimani used Iranian-state-owned businesses and banks as virtual cash machines to fund and support his terrorist activities, and those of proxy groups including Hamas, Hezbollah, and al-Qaeda. To think that Soleimani was not planning or actively trying to kill Americans at the time of his death is to deny or ignore everything he had done in Iraq for years preceding his death. Soleimani spent those years zealously targeting Americans and killing them—more so than any single individual terrorist in recent times.

IMPACT ON U.S. SERVICE MEMBERS, CONTRACTORS, AND THEIR FAMILIES

Indeed, Soleimani was an expert at death and destruction. In April 2007 I had just returned from a 13-month tour of duty as the deputy commanding general of U.S. Forces in Afghanistan and was appointed as the deputy director of the Joint Improvised Explosive Device Defeat Organization—responsible for training the force, defeating enemy IEDs, and attacking enemy IED networks. Accordingly, we had operations and intelligence cells State-side and in both the Iraq and Afghanistan theaters of operations.

Soleimani developed, refined, and deployed explosively-formed penetrators (EFPs)—lethal roadside bombs made of an Iranian-milled 6-inch copper disc, PVC/steel pipe, urea nitrate, a blasting cap, and typically, a passive infrared switch trigger. When a target crossed the beam of the passive infrared switch it ignited the blasting cap which in turn detonated the explosives, propelling a molten copper disc at 8,000 feet per second through its mark, killing and maiming whoever might be in the projectile's (and its many fragment's) path of destruction. Frequently the destruction from an EFP sealed the vehicle doors shut, leaving American soldiers to burn alive. Often Soleimani's EFPs were deployed in multiple "arrays" where several copper discs would punch through Humvees and other fighting vehicles, ripping arms and legs from servicemen and women. Soleimani and his chief lieutenant Muhandis were the masterminds behind, and suppliers of, the EFPs. Soleimani and his terrorist proxies spearheaded Iran's efforts to inflict death and destruction on Americans in an attempt to disrupt American foreign policy objectives in the region, and to deny the Iraqi people a free and democratic Iraq.

---

[3] Iranian Charged in Terror Plot, *The Washington Post,* Jerry Markon & Karen DeYoung (October 12, 2011); and Iranian agents once plotted to kill the Saudi Ambassador in D.C.—The case reads like a spy thriller, *The Washington Post,* Reis Thebault (January 4, 2020).

[4] U.S. Attorney's Office SDNY Press Release: *Hizballah Related Money Laundering Scheme,* December 15, 2011; and U.S. Attorney's Office SDNY Press Release: *Manhattan U.S. Attorney Announces $102 Million Settlement of Civil Forfeiture and Money Laundering Claims Against Lebanese Canadian Bank,* June 25, 2013.

The Department of Defense reports that, at least, 602 brave Americans were killed by Soleimani's lethal IEDs. While accurate, that number is misleading. For every casualty there are historically ten-fold wounded. The math then suggests that Soleimani killed and wounded over 6,500 American servicemen and women. Even that number in no way captures the costs to tens of thousands of American spouses, children, parents, and communities all ripped apart as if they themselves were hit by these gruesome bombs.

IRAN AND SOLEIMANI RESPONSIBLE

Just in the last 18 months, two U.S. Federal judges each separately found Iran liable for their role in killing and injuring Americans in Iraq by providing material support to Iran's proxy terrorist groups. Those U.S. District Court cases are *Karcher et al* v. *the Islamic Republic of Iran* and *Fritz et al* v. *the Islamic Republic of Iran* (attached).** Evidence in both cases proved that Soleimani and Muhandis, both senior leaders in Iran's IRGC Quds Force acted on behalf of Iran to ensure Americans would die. Both of these cases introduced expert witness testimony from combat veterans on the front lines in Iraq that describe Iran's role in supplying EFPs to Iraqi militias that were carrying out these brutal attacks. I submit these 2 Federal district court rulings and refer to just a few quotes of supporting expert witness testimony[5] buttressing each:

- Former CENTCOM commander General David Petraeus said at an MNF–I press conference in April 2007: "And there's no question, again, that Iranian financing is taking place through the Quds force of the Iranian Republican Guards Corps (to Iraqi fighters)."
- Former Division and JIEDDO commander Lieutenant General Mike Oates said: "In fact, one of Iran's primary forms of material support to the Special Groups was financing, manufacturing and deploying EFPs."
- The State Department issued a country report that stated: "Iran's Qods Force continued to provide Iraqi militants with Iranian-produced advanced rockets, sniper rifles, automatic weapons, and mortars that have killed Iraqi and Coalition Forces as well as civilians."
- Dr. David Gartenstein-Ross, said of Muhandis: "Muhandis was given Iranian citizenship in the 1990's, and became an advisor to IRGC–QF commander Qasem Soleimani. Muhandis returned to Iraq in March 2003 and created Kata'ib Hizballah in 2007."

AUTHORIZATION OF USE OF MILITARY FORCE

As they were moving freely about the region coordinating terror with Hezbollah and Shi'a militias in Iraq, Soleimani and Muhandis presented themselves in a designated combat zone[6] as the leaders of designated terrorist organizations, the Quds Force[7] and Kataib Hezbollah. President Trump responded appropriately under the same Authorization of Use of Military Force[8] that President Obama used against state and non-state actors in Iraq, Syria, Afghanistan, Yemen, the Northern Tier of Africa, and other locations. Indeed, Iran never stopped attacking U.S. interests in the Middle East even after the Iran nuclear deal. Given Soleimani's assistance to al-Qaeda in the immediate aftermath of the 9–11 attacks, the strike on Soleimani was especially consistent with the AUMF. Indeed, President Trump's strike was part of our National security strategy of pursuing terror "threats to their source."[9]

IMMINENT THREAT

Commanders with combat experience leading servicemen and women in harm's way are required to make life-or-death threat assessments as part of their job. Threats requiring decisive action are usually kinetic and complex, derived from a vast array of information and intelligence that needs to be considered holistically, often times in a matter of moments. The forces loyal to and commanded by Soleimani and Muhandis had already attacked and killed an American interpreter and wounded 2 soldiers with rockets, and then subsequently attacked the U.S. Embassy in Baghdad. Whether larger successive attacks were minutes, days, or weeks

** Attachment A has been retained in committee files.

[5] *Karcher, et al.* v. *Islamic Republic of Iran* Case No. 1:16–cv–00232–CKK (Aug. 26, 2019); and *Fritz et al.* v. *Islamic Republic of Iran* Case No. 1:15:cv–00456–RDM (August 2, 2018).

[6] Executive Order 12744 (The Arabian Peninsula Areas).

[7] Executive Order 13224.

[8] AUMF, Pub. L. 107–40, codified at 115 Stat. 224 and passed as S.J.Res. 23 by the U.S. Congress on September 14, 2001.

[9] *National Security Strategy,* President Donald J. Trump, December 2017.

from happening, the fact that Soleimani/Muhandis-led terrorists had already attacked the United States twice in a matter of days, coupled with their Commanders' battlefield presence and their long and malevolent pasts, underscores the very imminence of a real and present threat. It would have been irresponsible for President Trump not to act. And he did so decisively and proportionally.

While serving as the deputy commanding general of U.S. Forces in Afghanistan in 2006 and 2007, I directed several combat missions to include drone strikes, artillery strikes, air assaults, and other operations, some of which found me on the ground with the soldiers conducting those missions. Everything I have seen, read, and understand regarding this strike underscores its legality, importance, and proportionate nature to reset the balance of power in the Middle East with respect to U.S. interests and Iranian influence.

REGIONAL STRATEGY

This administration's policy and strategy in the region is well-stated in the National Security Strategy document published in December 2017, and in multiple open-source commentaries. I will summarize by saying broadly the strategy is to:

- Stop Iran's drive to hegemony in the region;
- Prevent their development of nuclear weapons;
- Disrupt their exportation of terror around the region and world;
- Coerce the Iranian government to stop oppressing its people;
- Root out terrorism at its source; and
- Protect U.S. vital interests in the region.

ELIMINATING SOLEIMANI MAKES THE UNITED STATES SAFER

The Soleimani strike is consistent with U.S. National Security strategy as it relates to Homeland Security. Specifically, the 2017 National Security Strategy highlights the administration's plan to secure the homeland by:

i. Secure U.S. Borders and Territory:
   a. Defend Against Weapons of Mass Destruction.
   b. Combat Biothreats and Pandemics.
   c. Strengthen Border and Immigration Policy.
ii. Pursue Threats to Their Source:[10]
   a. Defeat Jihadist Terrorists.
   b. Dismantle Transnational Criminal Organizations.
iii. Keep America Safe in the Cyber Era.
iv. Promote American Resilience.

By definition, if we are concerned about Iran exporting terror either to the Middle East or to the United States, if we eliminate their chief exporter, Soleimani, then we have disrupted their operations, if not dismantled them in the near term. The Quds Force is tightly aligned with Hezbollah and its far-reaching terror tentacles around the world. They were a threat 40 years ago and they are a threat now. As has been our strategy for the last 2 decades, we must find these threats as near to their wellspring as possible and eliminate them.

Practically, in my roles as an education leader here in Washington, DC and in North Carolina, as Secretary of Transportation of North Carolina, and now as a chief executive with Air Data Solutions, an infrastructure and agriculture imaging company, I have been steeped in analysis of threats to and responsibility for specific homeland infrastructure and citizens over the last 10 years.

That Iranian sleeper cells exist in the United States is a matter of record.[11] Soleimani's death has created confusion in the Quds and Hezbollah terrorist command-and-control networks and impacts the resourcing of terrorist operations abroad. Similarly, when we kill a high-value target such as Soleimani or Muhandis, their fellow terrorists begin communicating and making mistakes. We most likely have new and actionable intelligence based upon the Soleimani strike. The idea is to keep the pressure on the enemy and never let up.

That notwithstanding, the Iranians have long persisted with "Death to America" chants and while I believe the Soleimani strike presents an opportunity for diplomatic opening, there undoubtedly will be Iranian hard-liners who wish to continue with the reign of terror. To that end, since prior to recent events, I have been and remain concerned about:

i. Cyber attacks on key infrastructure such as airport air traffic systems;

[10] Emphasis added.

[11] Iranian Charged in Terror Plot, *The Washington Post,* Jerry Markon & Karen DeYoung (October 12, 2011).

ii. Physical security of soft targets such as schools and mass transit for shock value;
iii. Attacks against seaports to impact commerce;
iv. Smuggling of weapons and other resources to enable attacks;
v. Biological warfare against crops affecting our food supply.

These are persistent threats, which with Soleimani gone will be much harder for Iran to execute. The strategy now should be one of continuing to engage Iran with all elements of national power, diplomatic, informational, military, and economic, to dissuade Iran from its long-standing predilection to kill Americans.

With Soleimani and Muhandis removed from the equation, we have an opportunity to positively reshape the dynamic in the Middle East toward peace and enhance homeland security. As a young United States Military Academy cadet in 1981 my classmates and I witnessed first-hand the return of the U.S. hostages in Iran to American soil at West Point where they spent their first weeks reintegrating. The cruelty of the Iranian Islamic Revolution is seared in my memory, and I am personally proud that we have begun to fight back.

Chairman Thompson, Ranking Member Rogers, and Members of the committee—thank you again for this opportunity to discuss my experience and views on this important issue and with respect to countering terrorism and protecting the homeland. I look forward to answering any questions you might have.***

Chairman THOMPSON. I thank all the witnesses for their testimony. I'll remind each Member that he or she will have 5 minutes to question the panel. I will now recognize myself for questions.

This hearing, "U.S.-Iran Tensions: Implications for Homeland Security" is titled because a lot of concern has been expressed as to whether or not with the recent incident in Iran are we in a safer or are we safe, or what should we look out for? So the question that I'd ask all the witnesses is, with those events of recent time in Iran, what do you believe is the greatest threat emanating from Iran today to the homeland?

Ambassador Leaf.

Ms. LEAF. Mr. Chairman, I think in the immediate term my biggest concern is the future of the, or the status of the U.S. military mission in Iraq for the reasons that I cited and that I went into greater detail in my written testimony. That is—the fight against ISIS is not over. The caliphate is gone but the attacks happen daily across Iraq and certainly there are thousands of ISIS members who have access to several hundred million dollars of monies for their attacks. So to the degree that we don't navigate the turbulence in Iraq well, we're going to see that mission pushed out. That mission goes directly to Homeland Security.

Chairman THOMPSON. General.

General STEWART. The question really is, is the missile attack against al-Asad—sufficient to say that we have done something and we can de-escalate and have a conversation. I don't believe that's sufficient to show the magnitude of the attack against Qassem Soleimani. So I expect that while not a direct terrorist threat to the homeland, terrorist threat globally has increased. If nothing else Soleimani controlled, and I use that term advisedly, controlled militias and the malign actors.

I don't know who controls those actors now. I don't know which ones will now say we have got to take revenge as a result of this activity. So I suspect that there will be some terrorist activity globally, time and place of choosing that requires a good bit of planning, but not directly to the homeland. The direct threat to the homeland is if the rhetoric continues and we decide to do some-

*** Attachments B–D have been retained in committee files.

thing in cyber space. There are vulnerable areas within our cyber environment both in the financial and the electrical power sector.

So if we're not doing everything to harden those positions, again, the uncontrolled, if not controlled or then the high-level activities by the Iranians, we could see activity in cyber space, and I'm very concerned about some vulnerabilities there.

Chairman THOMPSON. Mr. Warrick.

Mr. WARRICK. Mr. Chairman, the possibility of a terrorist attack by Iran here in the homeland is that: A possibility. But cyber attacks are a certainty. Equally certain is that Iran is going to continue its disinformation operations and, as well, that Iran is going to find ways to try to divide Americans, increase divisions and conflict within our society as Russia and China are already doing.

I also do want to agree with Ambassador Leaf and go more to the point that if Iran succeeds in forcing the United States to withdraw from Iraq on Iran's terms, rather than on our own, that will be a victory that we will be paying for for many, many years. Finally, I also agree that the possibility of ISIS staging a resurgence is also a certainty. The question is whether U.S. forces are going to be able to contribute to trying to prevent that from happening.

So that poses a long-term danger to the homeland that we have to take into account.

Chairman THOMPSON. General.

General TATA. Mr. Chairman, the revolution in Iran, they have been chanting death to America for 40 years. So I look at threats: Are they willing and are they able? Certainly, they are willing and they will remain willing as long as the theocracy rules Iran. So the motivation to harm Americans has not really changed in 40 years, and the motivation to export terror has not really changed in 40 years. What, what we have to look at is what is their capability, willing and able.

They're totally willing. Now, are they as able today as they were before January 2, and my contention is with Soleimani removed from the battlefield, and Muhandis—we don't mention him a lot but Muhandis was a critical player in Iraq—with those 2 people, the leadership matters. I'd liken it to removing the queen off the chessboard. He was somebody who moved around diagonally, straight forward, backward, to make—to ensure that Iran was enabling its campaign of terror to disrupt U.S. interests, vital interests in the region.

With him gone, we have an opportunity now and Iran knows how important he is, or was to their efforts. I believe that we have an opportunity. The individual who has replaced him was in the Afghan theater for Quds Force, not as familiar with ISIS, not as familiar with the Iraq theater of war, much less capable, doesn't have the elan that Soleimani had. I believe that we have got an opportunity now to have a diplomatic outreach.

Chairman THOMPSON. I now recognize the Ranking Member of the Full committee, the gentleman from Alabama, Mr. Rogers, for questions.

Mr. ROGERS. Thank you, Mr. Chairman. We have all seen over the last few days the massive protests in Iran and for the first time they are not chanting death to America and Israel. They are pointing the figure back at the government, in part because my under-

standing is the economic pressure they are under there, which they are just going to be exacerbated now by our European and other allies who are talking about implementing sanctions because of the shooting down of the airliner and then trying to aggressively cover it up.

Theocracies always care about self-preservation more than anything else. Given this new level of tumult in their country, do you think that is going to heighten the chances of them striking out at us, or striking out at those protestors? What consequences would that have to our homeland security here?

General TATA. Ranking Member Rogers, I, I think the fact that they are a theocracy, I think the fact that they are, as you mentioned, are concerned about self-preservation, primarily what they will try to do is preserve their regime. So as we look at what their capabilities are, as I mentioned they are willing, they want to—it is good for their business to chant death to America and try to eliminate Israel and have that as their stick, so to speak. It is good for their theocratic ideologs of—that, uhh, follow them, and how that translates into capability; they're very capable, particularly with the $26 billion defense budget that they've had this past year.

So what we need to do is understand that the threats remain because they are still willing to do it. We have to do an assessment of the threats and in light of the Soleimani strike. What is their capability? Command-and-control is a key fundamental factor on the battlefield, and it is a life-long key factor. You know, Sun Tzu talks about it all, the clause of which, et cetera, and this is something that we really must take into account, is what is the future of Iran's Quds Force going forward?

As we kill enemy leaders, they also light up the network and begin to talk, and make mistakes, and it provides new intelligence for us. So we need to have, right now, a massive intelligence-gathering operation, which I'm sure we do, that picks up on all of the dynamics going on in the Middle East between Iran and all of its proxies so that we can build target folders and continue to keep the pressure on the enemy.

Mr. ROGERS. Now, in response to the Chairman's question, which I think is the key question for this committee in this hearing is, you know, what vulnerability do we have to the homeland from Iran, and pretty much uniformly you all said cyber threats. Going back to my point about the economic pressure and the domestic political pressure that the Iranian threats have, do they really have the economic capability to put behind a serious cyber attack on our country?

Mr. WARRICK. Mr. Rogers, they do and that is because they choose to prioritize expenditures on things like the IRGC Quds Force instead of the things that would make investments that would help their own people.

Mr. ROGERS. You think that will continue even given the economic pressures they are having, and the protests in the streets. Now, it seems to me at some point to just preserve yourself, you have got to start shifting that money back to let them have services again and money to buy groceries and things to be able to keep your power.

General STEWART. The cost of entering the cyber space is pretty low.

Mr. ROGERS. Is that right?

General STEWART. If you can identify malware and you can—even if you get limited amount of help in dissecting malware, you can turn that into a tool that you can use.

So the entry into this space isn't high. We are not talking about millions and billions of dollars, but a fairly low-cost——

Mr. ROGERS. From what we have heard from other panels, the cost for defensive capabilities is pretty high. That is one of the reason—and you have talked in—Mr. Warrick talked about we need to put more money behind our defensive—more assets. So it sounds like the offensive threat is less expensive than the defensive capabilities.

General STEWART. Well, the risk to their networks, it is pretty expensive to defend that, but to develop a capability that could be deployed whether for intelligence gathering, for disruption or for decisive defeat action, that cost is not terribly high. Now, they made a commitment to building their own intranet, building their down defensive capability. That was their first priority, but in terms of delivering offensive capability, that cost isn't terribly high.

Ms. LEAF. Mr. Rogers, if I could just address another element of your question.

I mean, the monies require, the budget require—first of all there is the prioritization as Tom Warrick noted, the prioritization of these asymmetrical tools including cyber, but also the proxies. If you look at Iraq or you look at Yemen—well, look at Yemen. That was a very low, small investment, high return in terms of the pressure that it put on Saudi Arabia, and the pressure it put on us indirectly. In Iraq those militias are 6—some of them go back to the 1980's, the Badr organization.

The others came up on the battlefield after the 2003 invasion, and during the fight against ISIS. They are parasitical. They are much like the IRGC, moving into the economic space and praying on the Iraqi financial bodies. So that is, again, a way that Iran does things on the cheap.

Mr. ROGERS. Thank you, I yield back.

Chairman THOMPSON. Thank you very much. The Chair recognizes the young lady from Texas for 5 minutes, Ms. Jackson Lee.

Ms. JACKSON LEE. Let me thank the Chairman and Ranking Member.

A byline that was cited by a number of news stations after the attack in Iraq on the soldiers was from a soldier that said "I was 100 percent prepared to die". To think as we relate to the issue of the impact on the homeland, we must also recognize the human impact and the deliberative responsibility of this Congress and the Executive to make informed, intelligent, and deeply strategized decisions. We are now living with the false information of weapons of mass destruction.

In the act of war, before the inspectors were even allowed to determine whether they existed, we now call Iraq the endless war. So Ambassador Leaf, I want to ask some questions and I will appreciate your indulgence of quick answers. I want to get to all of the panelists. I'd like think that the American people, I'll declare, do

not intend to support going to war with Iran. But what do you foresee as the next direct military conflict between the United States and Iran?

Ms. LEAF. Given the way Iran goes at conflict, which is the so-called gray zone, not head-to-head conventional conflict, it will revert to form. So attacks on shipping, cyber, et cetera, against partners. I don't see the immediate quest to take a strike at the United States because they are outmatched, but they will put pressure, they are putting pressure through Iraqi militias. That is where the battlefield is. So I don't see a strike as such being the most likely prospect.

Ms. JACKSON LEE. Do you think in using proxies, such as the Shiite group and others, could provoke the United States, however?

Ms. LEAF. That's a question I really can't answer, but it appears that the administration has settled on a line that if an American is killed, that will elicit a response.

Ms. JACKSON LEE. So we have the potential for escalation?

Ms. LEAF. Yes, as I said earlier, I do believe we are at a pause, but we are still in an escalatory cycle.

Ms. JACKSON LEE. It is clear that the President made false statements about the Obama administration giving $250 billion or $150 billion when those were dollars that had been retained, and they were Iran's dollars. So it is important to have accurate information to the American people and in the process of deliberation.

Lieutenant General Stewart, you said Iran's fastest growing audience being Russia, China, and U.S. allies in the region. Can you please clarify how you see their potential involvement and also the detriment to those, particularly the allies, in the region including Israel, Kuwait, Jordan?

General STEWART. Congressman, I think probably more than anything else the idea that we are not acting rationally and that they are conforming to international norms, is the message and themes that they are trying to get to our allies, and some of our adversaries. That we, Iran, are more stable and more deliberative in our process. We won't escalate. We will conform to agreements. We want to reduce the violence. None of which are particularly true, but those are the messages and themes that they are pushing to our allies——

Ms. JACKSON LEE. That'll be part of the false narrative as well as saying we'll stand by you when the United States will not.

General STEWART. That——

Ms. JACKSON LEE. That one of——

General STEWART. That's certainly part of the messaging.

Ms. JACKSON LEE. That only promotes danger for our soldiers, for the United States. Mr. Warrick, we are all concerned about cyber attacks. I sit on the subcommittee dealing with that on this full committee, and so give us—you gave us really a good explanation, but give us a deep dive into how far into the cybersecurity system that can impact the average American if Iran chose to do so.

Mr. WARRICK. Representative Jackson Lee, the first thing to remember is that cyber attackers are looking for an open door. So in an open society like the United States, in effect, all of us who have a computer, who have a home network, who have a small business,

are now on the front lines and are subject to potential attack from a country like Iran.

What this means is an entirely new dynamic. It is no longer sufficient for us to guard our military bases, or our Government buildings. We now have to figure out an entirely new strategy to work with the entire American public to educate the American people on our collective responsibilities. This is going to take, I think, an entirely different and stronger approach that I would hope would be led from the White House, in a way that makes improving our cyber defenses a National goal, much like civil defense was a bipartisan National goal in the 1950's.

Chairman THOMPSON. The gentlelady's time has expired.

Ms. JACKSON LEE. I thank you. Yield back.

Chairman THOMPSON. The Chair recognizes the gentleman from North Carolina, Mr. Bishop for 5——

Mr. BISHOP. Thank you, Mr. Chairman. Thank you all for being here.

You know, specifically, focusing on the purpose of today's hearing, there have been a number of claims in public and even maybe implications in some of the statements by Members today that there was a lack of planning by the U.S. Government including, perhaps, DHS for the aftermath of what happened in Iran. I wonder is there anybody on this panel—we have heard a confidential briefing, but is there anybody on this panel who is intimately familiar with the details of the Department of Homeland Security's planning or lack thereof?

Mr. WARRICK. Well, I believe, Representative Bishop, that would be me, but I am not going to get into any discussion of any Classified matters at an open hearing. Obviously you would want to hear from the people at DHS who are currently working those matters, as I left several months ago.

But as I know you have been briefed and as DHS leadership has said, they are quite a few activities, operations that are under way now that the Department is engaged in to try to help protect the American people.

I have no quarrel at all with any of those. Quite the contrary, I think they are excellent. I just think that there needs to be more of them and better funding from the Congress.

Mr. BISHOP. So to follow that up, Mr. Warrick, are such efforts, as a general practice, of long-standing, that is to say they don't just—aren't brought up in a crisis, but they as a matter of fact are pursued on a regular programmatic basis?

Mr. WARRICK. The Department realized after the Arbabsiar attack in 2011 that DHS had more actions going on against Iran than almost anybody else in the Government realized. I do have to say that that attempted terrorist attack on U.S. soil met with a very vigorous response from the Secretary of Homeland Security at the time and the entire Department leadership. I was very proud of having been involved in that effort.

Mr. BISHOP. Thank you, sir. General Tata, you said in the course of your comments that you have to do an assessment of threats. Would it be your expectation that those assessments would be ongoing as a matter of course over a long period of time and not just started in response to a crisis?

General TATA. That is correct, Congressman. The threat assessment cycle is one that is continuous, and it happens for overseas threats and for homeland security threats. The planning is all nested with the National security strategy that the President and the National Security advisor put out 2 years ago, and it very clearly talks about pursuing threats to their source and defeating terrorists, and defeating transnational criminal networks. So that is where you see DOD and DHS in the joint planning collaboration that happens where they assess threats and develop plans to counter those threats.

Part of that planning is to fight the enemy on their 5-yard line and wherever they may be. Part of it is to defend our 5-yard line to use a football analogy.

Mr. BISHOP. Thank you, General. General Stewart, in your testimony you talked about Iran's objectives and its asymmetric activities. One was to avoid the threshold for an overt U.S. action. It would appear that Iran miscalculated in this particular case. Wouldn't you agree?

General STEWART. Specific to the missile strike on the bases?

Mr. BISHOP. Yes, sir.

General STEWART. I don't think that was a miscalculation. I don't think Iran views that as a miscalculation. I think they viewed that as a demonstration that they would strike back, an overt demonstration that hit targets that they could reasonably tell their audiences that "we have done something".

Mr. BISHOP. Well, I think what I am getting at, and I am not sure if I am following you General, I am talking about the strike on General Soleimani and the killing of him. Do you think—are you saying that you think Iran anticipated that the United States would do that or did they miscalculation——

General STEWART. Not at all.

Mr. BISHOP. OK. All right.

General STEWART. Not at all.

Mr. BISHOP. One other thing is that you said that the most important information operation they have is on their own domestic population, which the regime seeks to keep united. Based on events of the last days, would you say they miscalculated on that as well and in the interest of accurate information, you know, I heard one public figure say that the killing of Soleimani is like killing Princess Di, or Elvis. Would you agree with that equivalence and do you think they have miscalculated in terms of their own population's reaction?

General STEWART. Their population reaction actually switched from a support to the reaction to the Soleimani killing but switched as a result of the airplane strike. So there is no way that they could have calculated that if we make an accidental shoot down of a commercial aircraft that the population would rise up in the wake of the cry for—the outrage over Soleimani's killing.

Mr. BISHOP. Thank you.

General STEWART. I don't know if I would call it a miscalculation. They are not dealing with it well and that causes some stress internally, but I wouldn't call it a miscalculation.

Mr. BISHOP. Thank you, sir. My time has expired. I yield back.

Chairman THOMPSON. Thank you very much. The Chair recognizes the gentleman from California, Mr. Correa for 5——

Mr. CORREA. Thank you, Mr. Chairman. First of all let me thank you for holding this most important hearing, and I'd like to thank our witnesses for being here today. Again, a very critical issue.

I have a question for all of you on the panel here. As you know, Iranian General Soleimani built the world's largest terrorist network with international terrorists like Hezbollah. Now that he is out of the picture, how would you characterize the threats posed by Iran's proxies, Hezbollah, Hamas, other militias, toward the United States and abroad? Do they have cells in the United States?

Is this a threat, especially given as some of you have stated, now that he is out of the picture, is there a call for revenge, and are there cells in the United States that could pose an immediate threat to us? Ambassador Leaf?

Ms. LEAF. Sir, I know that Hezbollah has cellular networks all over the world and I think it is clear that they have them in the United States. To my knowledge, this does not extend to some of the other proxy actors, but I think it is important to note, going back to your original question, that the Quds Force will survive, has survived, will survive and continue on the mission that Soleimani—the vision that he defined for the region.

Certainly it was a decapitation and Esmail Ghaani, his successor, is a character of a different type, but I have no doubt that they will exercise the kind of command and control throughout their networks, whether it is Hamas, Hezbollah, and certainly in Iraq in such a way that our interests will be threatened.

Mr. CORREA. So Ambassador, are you saying that command and control, despite his elimination, is still there and therefore there is discipline in the ranks?

Ms. LEAF. Certainly in Iraq, yes.

Mr. CORREA. In the United States, the cells?

Ms. LEAF. These—well, I'm going to defer to Tom Warrick on the issue of Hezbollah.

Mr. CORREA. Thank you. General Stewart.

General STEWART. I don't know—I won't speak to cells here, but the estimates are 20- to 80,000 members make up this militia, 20- to 80,000. Some of them will remain under command and control of the IRGC Quds Force. My greater concern are which of the ones that will go rogue with the intent to avenge the death of Soleimani, the martyred Soleimani.

Mr. CORREA. That's a question mark?

General STEWART. That's a question mark. I don't know how many, but even if a small percentage——

Mr. CORREA. Mr. Warrick, I'm running out of time. Excuse me, General.

Mr. WARRICK. So there was the recent disruption of a Hezbollah group including one of their sleeper operatives. It would be foolish of us to assume that by taking one out that there aren't others that need to be addressed by the FBI at the proper time and place. I do agree though with General Stewart and with Ambassador Leaf, that the Iranians would regard it as a ruthless but "good at a trade" if United States were forced by Iran to leave Iraq, if all they thought they had to pay was the price of one of their generals, I'm

afraid the ruthlessness of the regime would make them think that was a good deal for them.

Mr. CORREA. General Tata.

General TATA. Yes, Congressman, it is well-documented by the FBI and Southern District of New York in open source, and other places that there are sleeper cells here in the United States both for the Quds Force and for Hezbollah financing. I referenced in my opening statement about the hundreds of millions of dollars that there were being laundered by Hezbollah in the United States, a case brought before the Southern District of New York, or by the Southern District of New York.

The FBI intercepting the plot by the Quds Force to attack a restaurant a few miles from here in Washington, DC. It would be naive of us to assume that there aren't other cells that we have not yet found. So they exist and as far as command-and-control networks of Quds Force, you know, you take out the—you destroy part of that network. Certainly they will regroup and reassemble, but you cannot overestimate the impact of killing Soleimani, in my opinion.

Mr. CORREA. General Stewart, we talked about the capabilities, cyber, offensive capabilities of Iran. Is there a possibility that they could team up with Russian experts and come up to a greater level of threat to the homeland if they were to do that?

General STEWART. In their own words, they have talked about partnering with a number of countries, to include the Russians, the Pakistanis. So in their own words they talk about sharing and collaborating. So if they do that they certainly can increase their capability.

Mr. CORREA. The Chair, thank you very much.

Chairman THOMPSON. Thank you very much. The Chair now recognizes the gentleman from Texas, Mr. Crenshaw for 5 minutes.

Mr. CRENSHAW. Mr. Chairman, thank you everybody for being here. I'll start with you, Ambassador Leaf.

You mentioned the importance of the mission in Iraq and that's a contentious issue across the political spectrum. Could you address directly why we have a mission in Iraq and address directly the, you know, the slogan of no more endless wars? Why are we there? What's the U.S. interest?

Ms. LEAF. The importance of the U.S. military training and advisory mission in Iraq goes precisely to a homeland security issue which is ISIS, which continues to regenerate in Iraq and of course across the border in Syria. So that is forthrightly the mission, and I think it is a critical one.

Now, the size, the shape, the duration and so forth is a question that we should have a very strong voice in. I agree firmly with what Tom Warrick said earlier. If we are seen to be pushed out by this collection of a militia-affiliated actors in Iraq, or the militias themselves, we are going to lose critical intelligence. The Iraqi security forces will lose critical training and assistance to be able to counter that threat that goes beyond their own homeland.

Mr. CRENSHAW. Related to that would be the question of Iranian influence in Iraq. If we were pushed out it would become an Iranian proxy state, if you will. Does that affect U.S. National security

and related to that question, do you see the PMFs becoming the next Hezbollah?

Ms. LEAF. So the way I look at it is Iraq is at real risk of becoming a militia state, and as such will again pose a threat to the security of not just the neighborhood, but more broadly in the region.

Mr. CRENSHAW. Mm-hmm.

Ms. LEAF. We don't want to return to Saddam's days when Iraq was a real threat all across the way. So there are a multiplicity of these militias. They are, as I said, predatory, parasitical. They are thuggishly repressing hundreds of thousands of Iraqis who turned out with a quest to turn Iraq into a normal state. Iraq is not fully normal yet and it is in our interests to stay the course and help them do that, not only through this military mission, but the military mission is a critical component of our reason for being there.

Mr. CRENSHAW. All right. I want to move on to General Stewart and information operations that you mentioned. You talked about the use of social media by the Iranian government to spread their misinformation campaigns. In the last couple of weeks, how have you seen any change in that and how have they used the hyperdivisive reaction to Soleimani's killing, and the media narratives out there, have they used that internally to spread their own misinformation campaigns?

General STEWART. I have not seen that yet but I anticipate that they are laying the foundations to use the divisiveness. They are laying the foundation for the divisions, the social divisions within our country. We have seen them talk about doing that.

Mr. CRENSHAW. Yes.

General STEWART. But in the last 10 days I have not seen an increase in that level of activity.

Mr. CRENSHAW. For both Mr. Warrick and General Stewart, as far as the symmetry that you talked about, does Iran currently have even close to symmetrical capabilities as far as offensive cyber warfare against the United States? Is there something you are worried about in the future? Are you worried about it now? Because it is not as if we don't receive attacks from Iran in the cyber realm every day.

Mr. WARRICK. But I—you are right on that, Representative Crenshaw, but it is a fact, as General Stewart said, that offensive cyber operations are cheap. Defensive cyber operations are very expensive.

Mr. CRENSHAW. I understand. I'm trying to get a sense of the capability as it stands now.

General STEWART. You don't have to have the same capability that the United States or Russia has. You only have to have one——

Mr. CRENSHAW. Yes.

General STEWART [continuing]. Can impact the electrical power grid on the east coast of the United States, and the cascading effects of that one device, and that is why it is asymmetrical.

Mr. CRENSHAW. I agree with that. I just—my question is it is not like they haven't tried, right? I mean in Texas we had 10,000 attacks. So are they not implementing their full capability yet? Is that your assessment?

General STEWART. Well, we call every event an attack.

Mr. CRENSHAW. Yes.

General STEWART. It might be reconnaissance.

Mr. CRENSHAW. Yes.

General STEWART. It might be simply probing. It might be an attempt to simply deface. All of those are precursors to "The Attack".

Mr. CRENSHAW. Right.

General STEWART. But generally, we are pretty cavalier about an event that occurs—an anomaly on a network and we can attribute it as an attack, and it doesn't mean that they don't have that capability and could, in fact, turn those probing events into a destructive event.

Mr. CRENSHAW. Mr. Warrick, you are very familiar with CISA and what they have been doing in the Department of Homeland Security. Is there anything they are not doing that you would suggest that they improve upon, because they have made quite a few steps in the last couple of years to improve upon cybersecurity in the homeland?

Mr. WARRICK. So if you look at the entire number of cybersecurity specialists that CISA has, that number would be dwarfed by putting 1 or 2 of our banks together with the number of cybersecurity people they have. So the staffing disparity of what is needed to protect the country is very different. This is one of the things that I would hope this committee and your colleagues on the Appropriations Committee would work together to address.

We have totally mismatched the idea of offense and defense, because in the military realm it means one thing. It is totally different in homeland security in cyber space.

Chairman THOMPSON. Gentlemen——

Mr. CRENSHAW. I am out of time. Thank you, Mr. Chairman.

Chairman THOMPSON [continuing]. From Texas' time has expired. The Chair recognizes the young lady from New Mexico, Ms. Torres Small.

Ms. TORRES SMALL. Thank you, Mr. Chair. Thank you, Mr. Ranking Member. Esteemed witnesses, I really appreciate you being here. I want to pick up on Congressman Crenshaw's questions about National security. I recognize that, you know, what is being said here is that that is the most likely attack we will continue to see. Mr. Warrick, you described it as a certainty at this point that we will continue to see it.

I am very interested in your conversation about a security gap that exists between Federal entities and some civilian entities. Most troubling of which are critical infrastructure and financial institutions. So my concern is, was you talked about opening a door and lots of attempts to open those doors, and such that all of us are now a threat. How do you see that impacting more rural utilities or smaller utilities, like water, wastewater, energy, and what can we do to address that threat?

Mr. WARRICK. So what the Iranians as other potential or actual cyber adversaries face is they literally try computer system after computer system until they find somebody that has not updated their software; that does not have antivirus software; that has failed to use two-factor authentication; that has failed to do all of the basic things that really need to be something that we start

teaching in America's schools. This needs to be done exactly in the way that we did the Civil Defense Campaign in the 1950's.

The difference then being that a nuclear attack was a horrifying possibility, but a cyber attack these days from our adversaries like Iran is an absolute certainty. So I would hope that this would get a lot more attention across the board and at all levels.

What would not be something that any of us as citizens would want to see is a very destructive cyber attack by an adversary that has achieved strategic surprise against us as the Iranians have shown that they can do, and that there would have to be something like another 9/11 committee, or dare I say it, even a Pearl Harbor committee that would look into how did we miss this.

I'm telling you right now Representative, that the mismatch between what CISA has in the way of resources and what the threat is, is a strategic vulnerability to the United States homeland.

Ms. TORRES SMALL. Mr. Warrick, thank you so much for that. I think looking long-term in terms of education, I think is very valuable. In terms of short-term and the staffing challenges that you described and the resources, again, I want to get back to rural and small utilities.

What kind of resources does CISA need? What types of expertise do we need to facilitate that type of outreach?

Mr. WARRICK. So the larger utilities, obviously, have more resources. The smaller utilities are more uniquely vulnerable but cover, as you know, large areas and therefore there is more at risk. This is very much a situation where ways have to be found, obviously, to do various risk-based measurements. CISA has a considerable amount of expertise in trying to do those risk-based assessments.

So I recognize there has to be prioritization, but I also recognize that our adversaries have very different prioritization and will look for the weakest target that they can find in a way of showing their dominance over us in cyber space.

Ms. TORRES SMALL. Thank you very much. Just shifting gears slightly, in the last time I have, in the event of a successful cyber attack against the United States, what is the likelihood of an attack being linked to the actual actor?

Mr. WARRICK. One of the challenges is that although the attacks take place in seconds, as General Stewart knows better than any of us, having been at CYBERCOM, it can take, you know, days, weeks, or months to try to sort out who is responsible. This is an asymmetry that we have to recognize and I don't think there is any substitute for.

I would defer to General Stewart.

General STEWART. Attribution remains a challenge, but we are seeing the actors who use certain techniques, certain tools, certain approaches. So it is getting a lot—I won't say a lot. It is getting easier to attribute, but it is still—I could give a tool to a proxy and that proxy could use that tool in multiple domains to get to the target which really makes it hard to define who does it.

Ms. TORRES SMALL. Are there specific resources that Department of Homeland Security could apply to increase the ability to correct attribution?

Mr. WARRICK. The least significant but most important is one that I know my colleagues have been asking for which is the ability to require American businesses who have been hit by a cyber attack to disclose relevant information to the Department so that they can begin understanding and assessing this.

General STEWART. The private sector believes that the Department has a lot more intelligence that can attribute to targets than we actually do. The reality is in the private sector there is tremendous amount of intelligence capability. How we share that data, and this is why it is so important as public-private partnership, the sharing of the data, the collaboration in real time, is critical if we are going to attribute and react in a timely manner.

Ms. TORRES SMALL. Thank you. My time is expired.

Chairman THOMPSON. Thank you very much. Just for the record, this committee led a bipartisan letter to the appropriators, got CISA $350 million more and we plan to go back again and say, based on some of the conversations today because we're still behind in terms of capacity. We can only get that capacity with investment. So——

Mr. WARRICK. Mr. Chairman, we want to thank as just private citizens, I thank the Members of the committee for doing that because that was hugely important.

Chairman THOMPSON. Absolutely. The Chair recognizes the gentleman from Louisiana, Mr. Higgins, for 5 minutes.

Mr. HIGGINS. Thank you, Mr. Chairman for holding this important hearing. I thank our witnesses for appearing today. I'd like to dive into the—some would say controversial killing of terrorists. I personally support the killing of terrorists in the battlefield, including President Trump's decision of order, precision, strike, to take out known and brutal terrorist Soleimani.

Iran is a threat to our homeland and continues to be the leading state sponsor of terrorists groups, and proxy terrorists groups across the world. They provide shelter and training for terrorists and intend us harm. They are no friend to the United States of America.

When I say, they, meaning an Iranian regime, not the Iranian people. One of my best friends, been my friend since 1984, is an Iranian citizen that was stuck in his country—he was going to college and when the Ayatollah Khomeini took over and the radicals took over Iran, he was stuck in the country. If he went back he will be shot. To this day, he can't go back.

So Iran, the Iranian regime is the issue and the threat they pose to our Nation, both our homeland and abroad, not the Iranian people. The Iranian people are beautiful people.

I have come to know their culture through my friend, but the Iranian regime is most certainly a terrible issue that we must confront. I think the—I am going to ask a question to Lieutenant General and the Brigadier General, both my generals. General Stewart, I'd like you to address, if you would, in your written statement you mention a divide between Democrats and Republicans with the narrative of how this thing is rolling, especially on social media.

You said that that is used by an Iranian as, "information operation targets". Can you explain in greater detail what that means, please?

General STEWART. Just like we have seen with other foreign governments who have taken every divisive issue, every divisive issue and then amplified it in a social media space so that long before we even cast a vote, we made a determination as to which side is telling the truth. We have seen this done by other nation states. We see this being done by the Iranians. Any—pick your socially divisive issue, any one of them.

Create an environment, and I won't call out any social media platform, create an environment, create the messages, drive people to those left and right lateral limits, and I have often said publicly and privately, I am not afraid of the Russians, the Chinese, the Iranians, or anyone else. I am concerned about the divide in our country and social media allows that divide to occur, and lots of us are amplifying those horrible——

Mr. HIGGINS. Well-stated and that division as it becomes manifest and publicly consumed on social media is a tool that Iran used to recruit, is it not?

General STEWART. I don't know how much recruiting they used that means, but they do cause disruption in our society and division in our society. It certainly could be used for recruiting.

Mr. HIGGINS. Thank you for that clarification. Brigadier General Tata, in your written statement you described that the world is a safer place because of President Trump's call to kill the known terrorist Soleimani. In your opinion, do you believe that we are prepared to counter any future attacks by his successors, although to some uncertainty as there should be? We shook them up regarding who that successor will be. Do you believe we are prepared?

General TATA. I do believe we are prepared. I think the intelligence and communications, and special forces, and combat force posture throughout the Middle East is appropriate and to defend U.S. vital interests which are defense of people, property, and the shipping lanes. Those are the key U.S. vital interests that we have, and of course to be able to root out terrorism at its source, to disrupt attacks on the homeland.

So as we in the days after, weeks, months after the strike on Soleimani, the key for us in my opinion is that we have to have an intelligence apparatus that can continue to collect information, so that we can make informed decisions about how to continue to disrupt the terrorists that want to do us harm. That to me is fundamental more than anything else going forward.

Mr. HIGGINS. Thank you for that answer and your clarification, and your service. Madam, gentlemen, thank you for appearing today. Mr. Chairman, I yield.

Chairman THOMPSON. Thank you very much. The Chair recognizes the gentleman from New York, Mr. Rose for 5 minutes.

Mr. ROSE. Thank you, Mr. Chairman for gathering this extraordinary panel. I must say as well whenever Mr. Higgins speaks, I always consider yielding all my time to him, but I will resist.

In the immediate aftermath of the killing of Qassem Soleimani, something that for the record I did support, there was a concern regarding reaching out to jurisdictions regarding a potential terrorist attack, cyber attack. As a New Yorker, we saw that there was a strong communication between the JTTF, NYPD, and DHS.

But what I'm concerned about is that we don't know what we don't know about our communications with other jurisdictions.

In your experience, does CISA, DHS, as a whole, do we have contacts with every locality? Have we built communications with every jurisdiction and do we have a means of at least grading whether they are up to a certain requirement, whether it be counterterrorism or cybersecurity? I'll begin with you Ms. Leaf.

Ms. LEAF. I think that really falls outside my bailiwick of expertise and I would defer to my——

Mr. ROSE. Of course, thank you.

General STEWART. I can't completely speak to this except for when I talk to industry partners who do not believe there is a great connection between their requirement at the, let's say a small or medium-sized bank, so the right connection within DHS to the right connection inside the IC. So from a commercial standpoint the sentiment is we are not well-connected. I don't know how the Homeland Security is connected to the municipalities and governments, but——

Mr. ROSE. OK.

General STEWART [continuing]. From a private-sector standpoint, they don't feel well-connected.

Mr. WARRICK. So to square the circle, Congressman, someone at DHS could show you a map that says that the entire country is covered by fusion centers; that the entire American economy is covered by sector groups that meet with specific sectors. That much is true, but the reality is how many people are there within those JTTFs and how many people are there within those sector groups to reach out to all of the American State and local law enforcement, private businesses, and others. That is what produces the gap, and General Stewart has correctly——

Mr. ROSE. Do you think that this gap is something that we should be trying to analyze and establish some type of metric?

Mr. WARRICK. I wouldn't spend a lot of time analyzing it. The gap has to be addressed in a very serious way and urgently, lest we find ourselves the victim of strategic surprise from somewhere.

General TATA. Congressman, as former secretary of transportation in North Carolina, I had a law enforcement agency. I worked very closely with emergency management in North Carolina. I worked very closely with the Department of Public Safety, the equivalent of DHS at North Carolina's level, the Department of Transportation's work with the Highway Patrol.

All of those entities have a fusion cell and emergency management, and we worked very closely with FEMA and DHS. What I saw a few years ago when I was in that position was close coordination between DHS, FEMA, and other law enforcement agencies such as the FBI.

Now, can everything been improved always? Yes. But at the time the infrastructure is there and so it may be time to rejuvenate that or to put some emphasis on that.

Mr. ROSE. Last thing, my last minute. Can you speak to the potential for, and I don't think this is considered nearly enough, the potential for a cyber attack combined with a lower-scale terrorist attack? Iran seems to have both capabilities, and do you see that on your threat landscape?

General STEWART. It is certainly in the realm of possibilities, but I don't see any indication of that and I think that would be highly escalatory which would be counterproductive for the Iranians.

Mr. WARRICK. It is also true that the people who do terrorist attacks, and the people who do cyber attacks from Iran don't talk to each other.

Mr. ROSE. Can you expand on that?

Mr. WARRICK. The way Hezbollah and the Quds Force have organized their terrorist activities is through very tightly-held stovepipes. This is a matter of public record. This isn't the least bit sensitive. If you look at the way the FBI and the Department of Justice detailed the actions of the Hezbollah sleeper operative who was recently convicted and sentenced to 40 years in prison, you can see how tightly-stovepiped Hezbollah kept its operatives.

Cyber attacks are done through totally different mechanisms. That is detailed in General Stewart's testimony and it is done through different mechanisms. It would be quite something if they could combine those. Let us hope they don't.

Mr. ROSE. Thank you. That's very helpful.

Chairman THOMPSON. Thank you. The Chair recognizes the gentleman from Pennsylvania, Mr. Joyce for 5 minutes.

Mr. JOYCE. Thank you, Mr. Chairman. Thank you for holding such an important hearing today.

It is no secret that the Iranian regime is no friend of the United States. If I could just briefly summarize the highlights from some of General Tata's comments today that we heard. General, you testified broadly that Soleimani was a specifically-designated terrorist, and his murder, his removal from our continent, from our world, from our lives, makes for a safer Middle East and a safer homeland here in the United States. I, for one, could not be in more agreement with this.

Soleimani was a terrorist who had the blood of hundreds of American soldiers on his hands. Weakness and appeasement of Iran by the previous administration left the United States in a weaker position in the region, and led to a deeply-flawed Iran deal. Under the current President, we have taken a different tack, pulling out and seeking to re-establish against this rogue Iranian regime.

General Tata, your testimony also highlights that Iran and its proxies have posed a threat for over 40 years. Why have the past strategies, including President Obama's nuclear deal, why have they failed to reign in Iran's hostile activities?

General TATA. Thank you, Congressman for that question. I think part of it lies in the fact that Iran is a theocracy and they will always, as long as they are a theocracy fueled by extremist—Islamic extremism, they will always want to annihilate and remove Israel from the face of the earth. They will always want to destroy America and Western values.

Fundamentally, they are in opposition with the West. So for my point of view, that will not change as long as they are a theocracy fueled by fundamentalist Islam. So the nuclear deal, you know, just this year we have the removal of the sanction to export arms that would come due and come out of the deal had it still been in effect.

In 3 years, they would be able to import centrifuges and ballistic missiles.

Five to 10 years to people in the Middle East is the bat of an eye, and it is something that they will provide a holding action while they continue to do things. The deal did not prevent them from conducting, obviously conducting terrorist attacks against the U.S. interests in the region. So it is this belief that we can conduct a deal with them, that will result in some kind of peace. What we can have is deterrence, detente, and, you know, establish a power to counter their power in the region.

Mr. JOYCE. General Tata, what additional steps—those deterrents that you bring to the table, what would you recommend that we utilize moving forward to secure our homeland and to mitigate additional threats from Iran?

General TATA. Thank you, Congressman. The additional steps I would recommend, I have mentioned a few, ensure that we have robust intelligence capabilities in the Middle East to be able to pick up on the movement of these proxy groups and to determine how Iran is going to try to conduct more influence operations, whether or not that is kinetic or cyber. Or, you know, and this administration is expert at pulling the levers of diplomatic information, military economic power and synchronizing them to achieve specific effects. So they need to continue to do that.

Where they struck with military precision, no collateral damage on a confirmed terrorist target and killed that target, removed him from the battlefield. Now we need to take a look at what lever of power can now be best applied to achieve our strategy that is wellstated in the National security strategy to achieve that strategy and move forward. Now that we have a deterrent effect in that region, maybe they will talk. Maybe they will come and achieve at least some sense of detente.

Mr. JOYCE. Thank you for your important information you brought to us today, and I yield my remaining time.

Chairman THOMPSON. Thank you very much. The Chair recognizes the gentlelady from Illinois, Ms. Underwood, for 5 minutes.

Ms. UNDERWOOD. Thank you, Mr. Chairman. Since the events in Iran I have been briefed by the Department of Homeland Security, the Department of Defense, the chairman of the Joint Chiefs, the Secretary of State, CIA director Haspel, and the acting director of National Intelligence. In the briefings I received information and intelligence regarding threats and the administration's efforts to keep us safe in the wake of the escalation.

As I have learned more about the administration's military escalations in Iran, the question for me is, are we safer? The answer after much listening, reading, studying, questioning, and listening some more is, no.

Americans and our allies are in greater danger. Our country is not safer in the wake of the Trump administration's recent actions. Without a doubt, General Soleimani got the fate he deserved and Iran remains an adversary. But after examining the facts, we are on less stable footing in the region.

The military has suspended counter-ISIS activities. More troops have been sent into a dangerous region. Iran is now closer to building a nuclear weapon than they were before the attack and we are

more isolated from our allies and partners. Ensuring the safety and security of Americans at home and abroad is my most important duty as a Member of Congress. In order to do that, I voted for the War Powers Resolution, and I pledged to work to keep our country safe from any counter attacks from Iran.

In response this administration's recent actions, we know that Iran is more likely to deploy asymmetrical operations on U.S. critical infrastructure and our allies. Because of this, the intelligence community continues to caution that a possible attack led by Iran, Iranian proxies would likely include a malicious cyber operation. Ambassador Leaf, General Stewart, and Mr. Warrick, as a nurse, I am concerned about how vulnerable our country's hospitals are as targets of cyber attacks.

What would a Wiper or ransomware attack look like if carried out on a hospital?

Mr. WARRICK. Representative, this would be one of the most serious attacks against any community, as we have seen from ransomware attacks that have been tried, including some that Iran has had its hand in. Any time you have a situation like that you are looking at the potential loss of patient records and ability to access medications, allergies, and other information that is necessary for the preservation of life and health. So this could be one of the most important types of targets an adversary might attack.

General STEWART. We continue to see adversaries look at the hospital system, and as Mr. Warrick pointed out earlier, we are all part of the attack surface because we all have a smart device of some sort. We plug into a Wi-Fi network that is unsecured. Almost every one of the devices in a hospital is on an unsecured network to allow folks to move laterally inside the network, steal data, disrupt systems. We are extremely vulnerable in the hospital and health care sector, and this is not just about stealing data. This is about impacting—we have hearing aids now that are Bluetooth-enabled.

Ms. UNDERWOOD. Right.

General STEWART. So all of our systems are connected and all of them create an attack surface from which you can move laterally and be disruptive. So I think this a really important area to focus on securing our health care infrastructure. It has been targeted. It is a high priority for all of our potential adversaries and criminals. So it is an area that I think we really need to invest in and set some standards for securing networks.

Ms. UNDERWOOD. Yes, sir. Ambassador Leaf, did you want to add anything?

Ms. LEAF. No, not on this topic.

Ms. UNDERWOOD. OK. What Federal resources are available for hospital administrators to proactively address cybersecurity vulnerabilities against a cyber attack from either foreign adversaries?

General STEWART. I can't speak to that.

Mr. WARRICK. Yes, there is advice that is available. There are tactics, techniques, and procedures.

Ms. UNDERWOOD. Mm-hmm.

Mr. WARRICK. But the problem is, of course, that implementing them is most often left to the communities that fund those hos-

pitals. It is not a subject of a massive Federal grant that somehow solves the problem. It has to be done at the State and local level in the communities.

Ms. UNDERWOOD. Right. So it sounds like it is an open vulnerability and, you know, General Stewart mentioned stealing data, but there is also interruptions in service delivery, threats to individuals' health and wellness. So this is something that I hope that this committee and our colleagues in Congress can address.

General Stewart, in your testimony you reiterate that the findings presented in the world-wide threats assessment of 2019 that, "Iran is also attempting to deploy cyber attack capabilities that would enable attacks against critical infrastructure in the United States and allied countries."

Can cyber attacks perpetrated by Iran and Iranian actors such as the ransomware attacks on Baltimore and Atlanta, provide insight into the potential scope and magnitude of future cyber threats from Iran?

General STEWART. So the ransomware attacks that we will see more of, by the way, it is a quick way to get funds. More and more companies are paying the ransom because they have seen the cost of Baltimore mitigating the ransomware attack. So these are criminal activities that could certainly be utilized by state actors to wipe data, to be disruptive and ultimately be disruptive on a network. So the techniques used for ransomware from the criminal standpoint are the same techniques that a nation-state could use to destroy data that they think is appropriate for disruption.

Ms. UNDERWOOD. Thank you. As I stated before, as a Member of Congress, it is my responsibility to ensure the safety and security of Americans at home and abroad. I am committed to working with my colleagues in the House and on this committee so that the United States is prepared for all contingencies related to U.S.-Iran tensions and I yield back. Thank you.

Chairman THOMPSON. Thank you very much.

The Chair recognizes the gentleman from New York for 5 minutes, Mr. Katko.

Mr. KATKO. Thank you, Mr. Chairman, and thank you panelists for being here. The discussion has been excellent and I think the testimony has been very well taken.

The situation in Iran has raised, what I think is the biggest vulnerability in our country, and I think—I just want to digress for a moment which I normally ask questions, I do want to make some observations then ask a question. I think the consensus is, is that the easiest and most, perhaps, effective way to fight back for state actors that are bad actors, or individuals across the globe that are bad actors, is cyber attacks.

I really do believe that we are having this discussion; we are talking about the things, talk about our concerns; we are talking about our vulnerabilities just like we did before 9/11, and we didn't do enough before 9/11 to stop what happened on 9/11. It is, to me, the biggest concern I have, is the vulnerability to this country from cyber attacks. I think since 9/11 we have done a very good job in the anti-terrorism field, not a perfect job but a much better job.

Look at the resources that we put into the post-9/11 era to make us safe from terrorist activities. Now we have this metastasizing

problem of cybersecurity. As I look at it, I do think it is the greatest threat to our country right now, for some of the reasons we discussed today. As I look at it, there is 4 areas I think we can focus on to really prioritize what we need to do. Then I want to ask a couple of questions on it.

First is cybersecurity proficiency is the smaller the business, the smaller the family, the less knowledge they have on the issue, the bigger the problem. Banks, of course, have whole departments like you know that—but, you know, a lot of businesses can't afford that. Therefore their vulnerability is amazing. Target's major security breach happened because of a heating and air conditioning contractor, gave the bad guys access into the system. That is what we have got to be thinking about. We are not thinking about it.

The emerging technology, some of us noticed. I think you noticed it. Lieutenant General with respect to, you know, Fitbits and the watches that we have. The internet of things is coming and the problems that that is going to pose for us. Every household in this country is going to have 20, 30, 40 devices that provide access to the internet and provide back doors to cyber attacks. So that is another thing we need to think about.

Even the supply chain issue with 5G technology and all of that. CISA and all CISA is doing. CISA is a young start-up company, basically, and they are doing a wonderful job under unbelievably difficult circumstances. The ISACs they develop Nation-wide have been wonderful, but it is not enough.

Then of course, you have on top of all that, you have let us beef this up. You already have a shortage of 330- to 400,000 employees, right now in this country for cybersecurity jobs. They project that with the next year or 2, or 3, there will be over a million-person shortage.

So how do you do that without drilling down and getting into the school curriculums like you suggested? So this is a huge problem and we have done, as a committee, I think a remarkedly decent job of addressing and trying to get funding to CISA, but it is nowhere near enough and it takes much more than this committee.

So with setting the doomsday scenario—I don't mean to do that, but at the same token, we have got to acknowledge, tomorrow if a bad actor wanted to flick a switch they could take out a grid somewhere. They could affect our water supply systems.

They are not doing it probably because we can do it to them, but also they probably view—that we would view it as an act of war. So with all that being said, what should we be doing? I know we are talking about the problems. What should we be doing to try and look at this thing holistically much better than we have right now? Mr. Warrick, I'd ask you first.

Mr. WARRICK. So Representative Katko, there is a lot that you have said I would certainly associate myself with. I think where we are as a country is that we have built an enormous part of our economy around an internet that simply grew up out of a series of decisions originally as a defense program that turned into something that frankly, you know, from 50 years ago we would have thought as science fiction. Now we all carry around in our pockets more computing power than what it took to get Americans to the moon.

But there has been no sort-of equivalent security architecture——

Mr. KATKO. That is right.

Mr. WARRICK [continuing]. To make that safe. This is going to require DHS, and FBI, CYBERCOM, the entire technology-related security architecture of the United States to figure out how better to work with the private sector. We don't want the Federal Government dictating standard and reducing innovation. That comes from a combination of public and private measures that frankly have made our economy vibrant. But something more has to be done on security.

One of the things that concerns me is that at DHS over the past decade since the Department was founded, we have added missions, and added missions, but we have not had resources added to match the missions that have been added. This committee, I know Mr. Higgins—I heard him at a hearing yesterday—make some important statements about the need for an authorization bill and one of the things I'd ask you all to look at is, is the Department of Homeland Security adequately scoped for the missions that it now has, because they are different from what the Department had when it was stood up in 2003.

We are, I think, at a fundamental mismatch between the security needs and what is funded by the Department and others to do right now.

Mr. KATKO. Mr. Chairman, I am out of time, but this is something I just think we have to spend a lot more time on it going forward.

Chairman THOMPSON. Well, and there is no disagreement. I think you will see some legislation proposed by Mr. Richmond to kind-of close the loop on some of those unmet challenges that we face as a country. The Chair recognizes the gentlelady from Michigan, Ms. Slotkin, for 5 minutes.

Ms. SLOTKIN. Thank you all for being here, for your testimony and for the conversation.

I am concerned, separate from the events that went on in the past couple of weeks, I am concerned about looking forward and making sure we are doing everything we can to protect ourselves and particularly to protect ourselves in our States, and back home. I am hosting a big call this Friday, just called Enhancing Readiness on Cyber Threats for my State and local folks, for everything from election officials to town supervisors.

I wondered if you could, maybe General Stewart, walk us through very briefly just to give people back home an understanding of how Iran is organized on cyber threats. You know, what does it look like? Is it someone in a headquarters? Is it a non-associated group under special cover? Just give us the literally 30-second version of how they are organized and perpetrate attacks.

General STEWART. By their own words they have somewhere in the order of 2,000 or so folks organized from a strategic level, through tactical levels, designed to No. 1, defend their networks, and No. 2, develop capabilities to go after any targets, partnering with nation-states. In their own words, again, we are looking for friends and partners friendly to us. They cited Russia, China, Pakistan, as friendly partners. So they are organized at the strategic

level. They are organized at the tactical level. They have specialized teams that conduct operations, both research and preparation for follow-on ops.

So they are well-structured throughout. They made a commitment to this effort over the last 10 years.

Ms. SLOTKIN. We know that in sort-of modern-day cyber warfare everybody is on this front lines. It is not traditional military or intelligence targets. We have talked about, you know, and I think Representative Katko, who has now departed, is absolutely right that one day the other shoe is going to drop, and we are all going to have this issue right in our face in a much more serious way. I know just as being a former CIA officer, after 9/11 we made a lot of progress on getting different intelligence community agencies to speak to each other, and to have better communication.

Then from the Federal down to the State and local law enforcement. But what kind of things should we be doing if we are thinking about the future of CISA and DHS, Mr. Warrick? What kinds of things should we be looking for and pushing for to now take it to the next level, so that we can be helping our businesses, small and large, protect themselves, since they are on the front lines?

General STEWART. Let me frame it this way. Sixty percent of small and medium-sized business fail within 18 months of a breach in cybersecurity. That is the economic underpinning of our Nation. Sixty percent will fail within 18 months. Insider threats are the greatest threat. So go back to how do we educate the population, because insider—all of the companies that have reported a breach, generally these are from the inside. They all have firewalls. They all have antivirus and it is some unknown entity inside that kicks off the attack. So we have got to do much better at coordinating at the National intelligence level, and I have seen significant coordination over the last 18 months.

The piece that I think is still missing—and I have mentioned this before—how do we move that from the National intelligence agencies, down to DHS, who are overwhelmed? I got to tell you, DHS does not have the number of folks——

Ms. SLOTKIN. Right.

General STEWART [continuing]. In order to carry out all of the missions that we have given them.

Ms. SLOTKIN. Right. So then let me just push you a little bit, because I have only a little bit of time, and maybe Mr. Warrick, you can answer this. Give us a vision of what "right" looks like. We have talked about how on a bipartisan basis this committee is very supportive of enhancing the resources that CISA and DHS has generally. Structurally, if you are king for a day, how do we get from where we are to a better place?

Mr. WARRICK. Every American citizen needs to realize that they are a source of cyber vulnerability or cyber resilience and strength. They see the Department of Homeland Security providing a coordinating mechanism that shares and assimilates the information that we give back so that if an adversary starts to attack us we can defend ourselves in microseconds. That is what the future needs to look like and boy are we not there right now. You are absolutely right.

Ms. SLOTKIN. I would just offer in my remaining couple of seconds that similar to Representative Katko, I think we have an interesting opportunity to speak as a committee about what we want to see proactively and I think CISA would welcome this, right, the opportunity to tell us how they get to "right" since they are not resourced the way they need to be now. I would welcome the opportunity for the DHS officials to come up here and offer those thoughts so that as we go into planning for next cycle we can give them the resources they need to protect us, or help protect us.

Chairman THOMPSON. We will. We have gotten a confirmation. The Acting Secretary is scheduled to come on March 3 to defend the budget. We will look at that. The problem most often comes is when someone will ask the Secretary, do you have all the money you need to keep us safe? He will, or she will generally say, I am here to defend the numbers. We are here.

So we get there but just like we put the additional $350 million in the budget for CISA last time, it was not in the budget but we put it there. So—and that was all of us working together to make that happen. So what I'm hearing now is that in a similar fashion we will have to kind-of take it on ourselves to do the right thing. Thank you.

The Chair now recognizes the gentleman from Mississippi, Mr. Guest, for 5 minutes.

Mr. GUEST. Thank you, Mr. Chairman. To our distinguished panel, thank you for being here this morning. I thank you for what you do each and every day to keep our Nation safe.

General Tata, you provided to us a written statement that lists forth in that statement what you describe as Soleimani's legacy of terror. In there you list that Iran has a $26 billion military budget and that for 3 years Iran, under Soleimani's leadership, has carried out 3 decades of terror against the United States. You go on to say that those include resources that Hezbollah has been provided to attack our allied nation of Israel in the Middle East.

It talks about him creating money-laundering schemes to fund terrorism; that following 9/11 that he was responsible for protecting the bin Laden family as well as al-Qaeda leadership. More recently we have seen Iran and General Soleimani be involved in the shooting down of drones, the seizing of oil tankers in the Strait of Hormuz, the attacks on the Saudi oil fields, the killing of an American contractor, and the recent attacks on the United States Embassy in Baghdad.

You go on to state that General Soleimani has killed or maimed more than 6,500 Americans and that he posed a clear and present danger to Americans' interests across this globe. You go on to say more so that he was more dangerous that Osama bin Laden himself. Then finally you close by saying that Soleimani's years of zealously targeting Americans and killing them made him more dangerous than any other terrorist in recent times. Do you believe that President Trump acted responsibly in authorizing the strike that killed General Soleimani?

General TATA. I do believe he acted responsibly, quickly, boldly, and it would have been irresponsible for him not to act.

Mr. GUEST. A matter of fact, you go on in your report to say not only was—did he act responsibly, but you said he also acted decisively and proportionally. Would you expand on that very briefly?

General TATA. Yes, so it was—if you see the pictures, obviously there was no collateral damage. The 2 high-value targets were killed which, by definition makes the command and control of those militias and back to Iran much more challenging for that state actor and the non-state actor. So, yes, it was under the use of authorization of use of military force.

Soleimani was heavily involved in the transporting bin Laden family and Taliban, and other al-Qaeda members immediately after 9/11. That's very well-documented and he hosted them in Tehran for several years afterward. He also moved Zarqawi from Afghanistan to Iran and then moved him into Iraq and resourced him. So there is no question that the AUMF applied to Soleimani and to Muhandis, quite frankly.

Mr. GUEST. General Tata, finally, as you close out your written statement, you say with Soleimani removed from the equation we have an opportunity to positively reshape the dynamics in the Middle East toward peace and enhanced homeland security. Do you believe that our homeland is safer today following the death of General Soleimani?

General TATA. I do believe the homeland is safer today because Soleimani and his, you know, morale-building, vast reach that he has is no longer. Any time that you take out such a leader with flare and élan and networks, and capabilities, and resourcing, there is going to be an impact. It may be weeks, months, years, but there is an impact.

It gives us this opportunity to exploit that impact and say to Iran we were serious about this. We will deter. We will defend and do not do this again. Do not allow for these networks to resurge and become the threat that they once were.

I believe if we do that we may be able to get a discussion going. We are going to be able to contain them, I think, and deter them. You know, until the theocracy is gone, I don't have any illusions that much will change as far as their willingness to do us harm.

Mr. GUEST. Finally, General Tata, do you believe and you say in your report that with the death of General Soleimani that this will help move the peace process forward in the Middle East?

General TATA. No, he was totally counterproductive to the peace process. That was part of Iran's two-pronged strategy was to pretend like they were deliberating in good faith and then to undermine all of our efforts in the Middle East, whether it is our interests with Israel, whether it is the interest in the Persian Gulf, whether it is our interests throughout southwest Asia by using Soleimani to conduct strikes.

So with him gone, we are safer, Congressman, and to add to some of the previous discussion, I would just say that in the homeland here I would hope that as we are doing legislation to make homeland security more robust, Mr. Chairman, that we would take a look at airports, seaports, railroads, energy systems and their vulnerabilities with regard to cyber, because now with Soleimani and all of them gone, this give us a two-pronged opportunity to re-

shape in the Middle East and also to make more robust, as the discussion here has led to, our homeland security.

Mr. GUEST. Thank you, Mr. Chairman. I yield back.

Chairman THOMPSON. Thank you very much. The Chair recognizes the gentlelady from California, Ms. Barragán, for 5 minutes.

Ms. BARRAGÁN. Thank you. Ambassador Leaf and Mr. Warrick, what consequences may result from the suspension of counterterrorism operations against ISIS and how should the administration be preparing for contingencies at home and abroad?

Ms. LEAF. Well, Congresswoman, it really depends on how long this goes and it goes back—endures, and it goes back to the issue I mentioned at the outset, which is it is quite critical for us to be navigating the turbulent waters in Iraq right now and that is quite testing. There is a hard push to get our mission out. It is incumbent upon us to signal very clearly, very consistently to—both privately and publicly that the cost to Iraq of that question, not just to us. But the cost will be significant. We will lose intelligence. We will lose the ability to have eyes on the problem.

Mr. WARRICK. Representative, every counterterrorism expert that you could get to come before this panel in or out of Government will tell you ISIS is planning a resurgence. The most dangerous thing I would say, speaking for myself, is a terrorist safe haven from which they can plan attacks, recruit, train, build capacity, and thereby threaten the homeland. So the terrorist safe haven is the thing we most need to try to prevent.

ISIS would like to establish one in eastern Syria or western Iraq, and that is a mission that I think we would neglect at our peril. So I—that would be the most important thing I think we need to be focused on, is trying to help the Iraqi government build up the capabilities so that it can do that mission eventually by itself. But they are certainly not there yet.

Ms. BARRAGÁN. Great. One of my concerns has been we have seen over the last several years a focus by the administration on immigration. It has been such a focus that it feels as though they have been taking away focus and efforts in other parts of homeland security and other departments. We have also seen the President diverting funds from the military to build his border wall. He has been diverting billions of dollars.

In September there was a report that in Virginia the State's cyber operations facility at Joint Base Langley will lose $10 million, just to give you an example. So here we are talking about cyber threats and we are talking about the potential increase, and there is money that is being diverted away from places like the cyber operations facility.

Does anybody on this panel want to comment about whether the diversion of any funds from places like the cyber operations could pose an additional danger, given that they have less funding?

General STEWART. Maybe it is built into my intel DNA that I am hesitant to comment on policy decisions, but any time you strip away capabilities, personnel, from an area like cybersecurity, that increases our risk and our vulnerabilities and risk. It is probably not something I would do.

Ms. BARRAGÁN. OK. Anybody else? I mean, I think generally speaking if you are investing less money into cyber operations, that

is going to result in less information and preparation. Is that accurate?

Ms. LEAF. I am not an expert in this, Congresswoman, but what I want to go back to is this issue of are we safer today. I do not believe we are safer today, because I believe this is but a pause in this cycle that we are in that we have been in with the Iranians for decades. One of the Members of the committee asked words to the effect of why did deterrence fail, when did it fail?

It has failed over a period of time and when you have a combination of this long-running cycle between the United States and Iran and you have deterrence that shreds over time, and specifically, I am looking back at last summer when the Persian Gulf provided sort-of a testing theater for Iran.

So I have no doubt that there is still payback to come from Iran notwithstanding that Soleimani is gone. He was the national hero. He was "like this" with the supreme leader. The supreme leader has put himself on the record that that missile strike is not enough. So cyber is the logical arena.

Ms. BARRAGÁN. Well, thank you. Thank you for bringing that up. That was going to be one of my next questions. Is this the end of the revenge phase?

I happen to represent the port of Los Angeles which is the busiest port. It touches every Congressional district and they have had their own attacks on cyber operations, and this just increases that ability. They can't just fend for themselves. We need—the Government is helping create some of these situations and making it worse. We need to help them and invest. Thank you all for being here and for your testimony. I am out of time. I yield back.

Chairman THOMPSON. Thank you very much. The Chair recognizes the gentleman from Louisiana, Mr. Richmond, for 5 minutes.

Mr. RICHMOND. Thank you, Mr. Chairman. Brigadier General Tata, let me just go back, and I am not trying to argue but I think there is some inconsistencies. You said that we are safer today because Iran was in the position to start selling weapons in a couple of years. They would be able to buy and import centrifuges and all those things and that they would never live up to a deal.

Then you went on to say now because of the killing and sanctions, that you believe that now is the time that they will enter into discussions. Well, either they are untruthful and they are never going to abide by a deal, or either they will. It is not based on who crafts the deal, whether it is President Obama or President Trump. Either they are good-faith actors or they are not. I have no reason to believe that they are.

However, I think we had the entire international community on our side under the Joint Comprehensive Plan. But let me ask another question. This is not a "got you".

I have 20 years in elected office and there is some things I hear over and over again that is just plain foolishness that makes us less safe. So one of the mantras from the other side is we have to do more with less. Can we protect more airports with less TSA agents? Anyone think we can? Does anyone think we can protect our internet, our local governments and our cyber space with less money or less employees?

General TATA. Well, Congressman, since you——

Mr. RICHMOND. Less resources?

General TATA [continuing]. Address to me I'd like to clarify something you said that I said which I said we are more safe today because we have killed Iran's chief exporter of terror, Soleimani and Muhandis, his chief executor of terror. So the—I believe that leadership matters and decisions matter with regard to capabilities. They are willing and able. They are less able today because the command and control of their chief terror network is gone.

Mr. RICHMOND. I didn't bring that part up. I just brought up the openness, willingness to honor and do a deal, but I want to be clear because I want the American people to understand that Government has responsibilities. Part of those responsibilities, we are not just tax-and-spend Democrats.

We want to protect the homeland and you can't do it with less resources. So what I am asking you all, please, raise your hand if you think we can protect this space with less resources.

Mr. WARRICK. Representative Richmond, no, quite the contrary. Secretary John Kelly, General Kelly, four-star marine with whom I had worked when we were both in Iraq and I proudly served when he was the Secretary of Homeland Security, famously told us in public and in private that the idea of doing less with less, or doing more with less, rather, is in almost all cases a fantasy. I would agree with Secretary Kelly on that view. I think as stewards of the purse of the American public it is your duty as Members of Congress to make sure that money is spent wisely and well, and that officials are held accountable for providing results the way American citizens——

Mr. RICHMOND. Reclaiming some of the time, but the point is that in this critical space more resources are critical success in defending our cyber space. They only have to get lucky once, and we have to be successful 100 percent of the time.

Let me ask you another question. Do you think that the lack of stability in terms of leadership at DHS causes some potential for concern?

Mr. WARRICK. Yes, absolutely. I am very concerned as all of us who have served in the Department know there are enormous advantages and especially when you come to the kind of strategic rethinking of the Department that can really best be done by senior officials and including political appointees who are confirmed in their positions by the Senate.

I would hope that as—actually, I believe it was Representative Higgins made this point at a hearing yesterday that this is enormously important for the Department to have more leadership confirmed by the Senate.

Mr. RICHMOND. Very quickly, to the two generals, do you think it is important, and do you think it is lawful for there to be a clear policy that answering cyber attacks doesn't necessarily have to be responded to with a cyber attack? I mean, can a cyber attack be so damaging to the United States that physical force response becomes appropriate and lawful? With that I yield back, Mr. Chairman.

General STEWART. I do not believe that the signal should be a cyber attack will result in a counter cyber attack. That all options should be on the table depending on the severity of the cyber event.

Though kinetic action is certainly appropriate as a response to the cyber attack.

General TATA. I agree with General Stewart.

Chairman THOMPSON. Thank you, very much. The Chair recognizes the gentleman from Rhode Island, Mr. Langevin, for 5 minutes.

Mr. LANGEVIN. Thank you, Mr. Chairman. I want to thank our witnesses for your testimony today as well as your service to the country. Before I begin my questions, I will say this on the issue of Soleimani. I don't regret for a minute that he is gone from the face of the planet. He was a murderer, a terrorist and a significant danger to the National security of the United States. The one problem I do have is with the overall lack of strategy, a strategic view of a strategy from this administration. That is the problem. They too often confuse tactical victories or decisions with somehow achieving strategic success and it doesn't always add up that way.

I hope in the long run that we are safer as a result of Soleimani gone. I guess we are going to have to wait to see over time. General Stewart, good to see you again. It took me a minute to recognize you with the beard, but looking very distinguished. I think you for your service to the country and the many years that you and I have had interaction together.

To you and Mr. Warrick, I want to discuss the Iranian cyber threat and trying to better coordinate between U.S. Government activities and the private-sector owners and operators of our critical infrastructure has certainly been a major focus of the Cyber Solarium Commission which I am currently serving which is charged with creating an overall strategic framework guiding policy document to help better protect the country in cyber space.

Do you believe that there are clear lines between what companies should be doing to protect themselves? What additional steps should they be required to do through regulation or incentives and what direct steps should the U.S. Government be taking to protect National assets?

Mr. WARRICK. So Representative Langevin, I mean, I am certainly familiar with the work of the Cyber Solarium, not as much as you are. At this point I don't think that there is enough of a clear understanding among the American people as to what are the responsibilities of the private sector compared to the Federal Government. I think where we need to end up is a better understanding upon all citizens as to what their responsibilities are, because I think people need to do more.

I think the Government is going to have to be a shared partner in a lot of these activities so that it is not so much the Federal Government telling citizens what to do, but citizens and the Federal Government, and State and local governments all working together toward a shared aim. We did that before in the 1950's on civil defense. We need to do it now.

General STEWART. We would not tell any organization in the private sector if a missile was in-bound on their target that since it doesn't impact that Department of Defense or the broader Government, good luck, you are on your own. That is basically what we told them in terms of—in cyber space. Good luck, you are on your

own. Do the best you can. Harden your defenses. The cavalry is not coming.

Mr. WARRICK. Oh, but here's a brochure.

General STEWART. Here is a wonderful brochure. Call the following numbers in the event of a crisis. How do we get from point defense to what General Alexander calls collective defense? That requires a sharing arrangement, where we are protecting our Classified but they are also protecting their proprietary information.

In many cases they are unwilling to share because it is proprietary that translates to share value. So how do we create the environment where we can seamlessly share intelligence at a high enough classification level in a timely enough manner, and they can share proprietary information and we have an environment where we have a good give and take between the private sector and public sector.

There are models, international models that are trying to do this including sharing information to the private citizens when they are under attack. We need to accelerate how we do that and the task forces are not necessarily the answer. They are not well-developed enough and I'll stop there.

Mr. LANGEVIN. Well, on that point, let me ask you this for your time at U.S. CYBERCOM and then also work at DHS respectively, what is your assessment of the interagency coordination when surging proactive cyber defense activities in response to either a direct threat or a general time of heightened tensions?

General STEWART. I have actually seen that improve significantly, Congressman. Now, I have been away for almost a year but in some of these specific targets that we have had an interest, I have seen the interagency collaborate. I have seen them plan. I have seen the increased authorities that U.S. cybercommand receives. So that interagency coordination looked like it was on the right path when I left the pattern in April. I don't know where it is today, but I saw a significant progress over the previous year or so.

Mr. WARRICK. While I certainly won't dispute the General's statement that there is progress, I do have a somewhat different perspective. It starts out from the idea that when offensive cyber operations are planned, the defensive specialists are often not in the room, and that kind of thing, I think, will have to be changed in the future, but that is a long-term problem. It is—we have got to understand, especially in the case of Iran that anything we do to them they will do back at us in some unusual way.

What we need to recognize is that they know when they have been attacked, and they don't care who attacked them whether it is us or somebody that may not be us. They can still take it out on us. So we have to have much better coordination between our offensive cyber warriors and our defensive cyber specialists.

General STEWART. If I can just build on that and I concur about having—it is important as we think the question, are we safer, that we listen to what the Iranian leadership says. The artillery strikes are not enough. They can't defend everywhere. Americans are more vulnerable to cyber threats than any other Nation because of their high level of dependency on cyber infrastructure. It is important for us to listen to what their leaders say.

General TATA. I would just add that in this continuum of Iranian tax since 1979 that are we safer, we have never been truly safe and the question is did the Soleimani strike affect their ability to carry out certain types of attacks. My contention is that it has.

Mr. LANGEVIN. Thank you all. Thank you, my time has expired. I yield back.

Chairman THOMPSON. Thank you very much. The Chair recognizes the gentleman from Texas for 5 minutes, Mr. Green.

Mr. GREEN of Texas. Thank you, Mr. Chairman. I thank the Ranking Member as well. I especially thank the witnesses for appearing today. Has the extirpation of General Soleimani created any unintended consequences that are adverse to our best interest, Ambassador Leaf?

Ms. LEAF. Congressman, I think that will take time to assess. With all due respect to my co-panelists, I don't agree that the Quds Force has really been dealt a significant blow. They are very resilient. I think there is predictability and method, and rationality to the way Tehran comports itself. So I—but the unexpected, I think you have to look a bit longer down the road.

Mr. GREEN of Texas. Are the consequences of leaving Iraq on our own volition the same as being evicted, Ambassador Leaf?

Ms. LEAF. Absolutely not. Look, I think it is very important to recall that within Iraq itself, there is a wide body of support that did not exist in 2011. There is a wide body of public support for us to say they well recognize it is not just a question of the counter ISIS fight and Iraqis are aware that they do not have that capability yet.

It is also—when we leave, the coalition leaves. There is a shrinking of engagement with Iraq. Iraq becomes more isolated, more vulnerable to Iran's pressure. Again, going back to the issue of what it becomes for the region and I assure you that our, that our partners around the region are looking carefully at this question, are we going to get pushed out, are we going to let ourselves get pushed out?

Mr. GREEN of Texas. Mr. Warrick, Nasrallah has command and control capabilities. He has probably one of the largest armies in the area that is not associated with a State. Is Nasrallah one of the rogue actors that you would be concerned with?

Mr. WARRICK. He is one of the most dangerous actors that we should concern ourselves with. He is not a rogue, but as both General Stewart and Ambassador Leaf said, the mission on which Qassem Soleimani was engaged in when he was killed in a strike was to build parallel state structures outside of the control of any government. That is a hugely dangerous proposition for the United States. This is what is creating the conditions that create forever wars. It is ironically not the United States. It is what Qassem Soleimani and his colleagues in the IRGC have been working on, and that is what makes it so dangerous.

Mr. GREEN of Texas. The word on the street, to use a pedestrian term, is that Iran received US$150 billion; that we gave Iran US$150 billion. Is it true that the money Iran received was money that we were able to deny Iran for some number of years?

Mr. WARRICK. Yes.

Mr. GREEN of Texas. It was Iran's money?

Mr. WARRICK. Yes, that is legally what it was.

Mr. GREEN of Texas. Is it true that the $150 billion is generally perceived by many, including the Treasury of the United States of America, as an inflated number?

Mr. WARRICK. So Representative Green, you happen to have hit somebody whose wife was in the office of foreign assets control at Treasury and has worked on this issue for more than 20 years. Those were assets frozen by Presidential order and were returned after a negotiation. So that is a simple legal description of what the money was.

Mr. GREEN of Texas. Thank you. I happen to have intelligence indicating that $56 billion is the amount the Treasury has tagged, but continuing with my very last question. Well, my time is up, but if I had the time I'd ask you about the safety of American citizens with reference to lone wolves who tend to act on their own emotions inspired by things that we can rarely understand, but I will not.

Mr. WARRICK. I would say that you would be right in your concerns that lone wolves are one of the most difficult things for law enforcement and homeland security to try to prevent.

General TATA. I would just add Congressman, that one thing that we should really look at is, why did the Iranian military budget grow by over 60 percent between 2015 and 2018 to $26 billion dollars?

Mr. GREEN of Texas. Thank you, Mr. Chairman. You have been more than generous. I yield back.

Chairman THOMPSON. Thank you very much. Let me thank the witnesses for your excellent testimony. I think you have gotten the committee in a good position to make some strong arguments from a budgetary standpoint that would help shore up some known vulnerabilities. We plan to use your testimony wisely in that effort. But we absolutely thank you for your forbearance on the questions as well as your timely response from them. So thank you very much.

Ranking Member—well, I ask unanimous consent to submit a statement for the record from the Jewish Federation of North America about homeland security concerns related to Iranian proxies.

[The information follows:]

LETTER FROM THE JEWISH FEDERATIONS OF NORTH AMERICA

January 15, 2020.

The Honorable BENNIE G. THOMPSON, Chairman,
The Honorable MICHAEL ROGERS, Ranking Member,
Committee on Homeland Security, U.S. House of Representatives, Washington, DC 20515.

DEAR CHAIRMAN THOMPSON AND RANKING MEMBER ROGERS: Thank you for holding this morning's timely hearing on U.S.-Iran Tensions: Implications for Homeland Security. As a major stakeholder for Jewish communal security, we wanted to share the following for inclusion in the record of today's hearing.

We understand that the FBI, DHS, and National Counterterrorism Center released a joint intelligence bulletin [1] in response to the recent escalation of U.S.-Iran tensions that directly pertains to Jewish communal security, as summarized below.

[1] JIB: Escalating Tensions Between the United States and Iran Pose Potential Threats to the Homeland, 8 January 2020 (IA–41117–20).

If the government of Iran (GOI) were to perceive actions of the U.S. Government (USG) as acts of war or existential threats to the Iranian regime, the GOI could act directly or enlist the cooperation of proxies and partners, such as Lebanese Hizballah. Based on previously observed covert surveillance and possible pre-operational activity, the GOI or its violent extremist supporters could commit attacks in retribution, with little to no warning, against U.S.-based Jewish individuals and interests among likely targets.

In recent years, the USG has arrested several individuals acting on behalf of either the GOI or Lebanese Hizballah who have conducted surveillance indicative of contingency planning for lethal attacks in the United States against facilities and individuals. In one instance, an agent of the GOI arrested in 2018 had conducted surveillance of a Hillel Center and the Rohr Chabad Center, Jewish institutions located in Chicago, including photographing the security features surrounding the Chabad Center.

Given the tenor of this assessment, we look forward to continuing to work with you and the committee to prepare and respond to all manner of international and domestic threats to the Jewish community.

Sincerely,

ROBERT B. GOLDBERG,
Senior Director, Legislative Affairs.

Chairman THOMPSON. I thank the witnesses again for their valuable testimony and the Members for all their questions. The Members of the committee may have additional questions for the witnesses and we ask that you respond expeditiously in writing to those questions.

Without objection the committee record shall be kept open for 10 days. Hearing no further business, the committee stands adjourned.

[Whereupon, at 12:26 p.m., the committee was adjourned.]

○