Iran’s Threat to
Saudi Critical Infrastructure
The Implications of U.S.-Iranian Escalation

By Seth G. Jones, Danika Newlee, Nicholas Harrington, and Joseph S. Bermudez Jr.

THE ISSUE
Tensions between Iran and the United States have heightened concerns about the threat to critical infrastructure in the Persian Gulf, including in Saudi Arabia. This report argues that while Saudi Arabia has vulnerabilities in its oil, desalination, electricity, SCADA, shipping, and other systems, Iran has thus far adopted a calibrated approach. Tehran has conducted irregular attacks to infrastructure using offensive cyber weapons, naval ships to impede oil tankers, and partners like the Houthis in Yemen. The United States should focus on deterring further Iranian escalation, refraining from actions that threaten the regime’s survival, and providing a political “off ramp” for Iran to de-escalate.

INTRODUCTION
There is growing concern about Iranian threats to Persian Gulf countries—particularly Saudi Arabia—as friction persists between Iran and the United States. Secretary of State Mike Pompeo condemned Iran’s missile program as “out of control” and a major threat to U.S. allies in the Persian Gulf. Senator Tom Cotton asked: “Can there be any doubt, any doubt that our partners in the Gulf are facing a genuine emergency as they fend off Iran? Oil tankers flying the flags of our allies and partners are ablaze in the Gulf of Oman.” And Saudi oil minister Khalid Al Falih lamented, “I am concerned though about the security of oil supplies from threats from state and non-state actors that we’ve seen. We’ve seen ships being attacked, we’ve seen pipelines being attacked, we’ve seen drones being launched from militias that are agents of Iran and that’s putting the global energy supply at risk.”

In response, the United States recently agreed to send more than 500 soldiers to Prince Sultan Air Base, extended the deployment of roughly 600 troops from a Patriot missile battalion, deployed an Air Force fighter jet squadron and a B-52 bomber strike group, expedited the deployment of the USS Abraham Lincoln strike group, and sent additional manned and unmanned intelligence, surveillance, and reconnaissance assets to the Middle East to counter Iran. As a U.S. Central Command statement explained, “this movement of forces provides an additional deterrent, and ensures our ability to defend our forces and interests in the region from emergent, credible threats.”

This CSIS Brief assesses the Iranian threat to Saudi Arabia by answering several questions. What types of strategies, tactics, and capabilities could Iran use against Saudi Arabia? What are potential critical infrastructure vulnerabilities in Saudi Arabia, and how serious are they? And what can the United States do to defend against—and deter—Iranian attacks against critical infrastructure?

The brief argues that Iran will likely rely on irregular means and actors, such as cyber operations and the use of partners like the Houthis in Yemen, to conduct attacks. If Iranian leaders feel further boxed in, however, they may take bolder actions. While there are significant
vulnerabilities to Saudi Arabia’s critical infrastructure, it would be difficult for Iran to cause strategic damage to most of these systems without escalating the conflict into a broader war that risks Tehran’s own critical infrastructure. Additionally, Saudi Aramco, Saudi Arabia’s national petroleum and natural gas company, has made considerable progress in protecting its infrastructure. But the Iranian threat remains serious.

The United States should focus on deterring escalatory Iranian strikes against Saudi Arabia and other Gulf partners by continuing to harden possible Iranian targets, as well as threatening and—if appropriate—conducting proportionate offensive actions in response to Iranian aggression. U.S. policymakers should also proceed cautiously in ways that don’t back Tehran into a corner, such as by threatening the survival of the regime, which might cause Iran to further escalate.

While Iran poses a threat to other Gulf states, including the United Arab Emirates, this report focuses on Saudi Arabia for several reasons. First, Iran and Saudi Arabia are major competitors for regional influence, a status which has been heightened by the Arab Spring and the wars in countries like Syria, Iraq, and Yemen. Second, Iran is more likely to target U.S. partners like Saudi Arabia than to attack the United States directly. Third, Saudi Arabia is a strategic target because of the Sunni-Shia rivalry and Saudi Arabia’s geographic position on the Red Sea, historic willingness to play a leadership role in regional politics, and oil reserves. Saudi Arabia has the second-largest proven crude oil reserves in the world, behind only Venezuela, at 267 billion barrels and 22.4 percent of global reserves.5 Saudi Arabia is also the world’s largest exporter of oil. Per day, it produces approximately 10.3 million barrels of crude oil and exports around 9.5 million barrels of both crude and refined oil products.6

The rest of this report is divided into three sections. The first examines Iran and its partners’ missile, cyber, and other irregular capabilities. The second section analyzes Saudi Arabia’s critical infrastructure vulnerabilities. Lastly, the third section outlines U.S. options to help protect critical infrastructure and deter Iranian escalation.

**IRANIAN AND PARTNER CAPABILITIES**

Iran possesses numerous capabilities that threaten Saudi Arabia’s critical infrastructure and maritime assets.7 This section focuses on several of the most important ones: missiles, cyber tools, and maritime anti-access/area denial capabilities.

**MISSILES**

All of Saudi Arabia is threatened by Iranian missiles, and the number of Iranian missiles capable of reaching the country would overwhelm virtually any missile defense system. Iran maintains the largest ballistic and cruise missile force in the Middle East, capable of striking targets as far as 2,500 km from its borders.8 Iranian missiles continue to improve in terms of range, speed, flight profile, and destructiveness.9 In the event of military escalation, Iran could use its largely road-mobile missile force to target critical infrastructure in Saudi Arabia and other Gulf states.10 Several of the sites highlighted in this brief—such as the port of Ras Tanura,
Ras Al-Khair power and desalination plant, and the Abqaiq processing and stabilization plant—exist within range of Iran’s land-based ballistic missile force. These sites are also vulnerable to ship-launched missiles. Targets further from Iran’s border, such as the refinery at Yanbu, located along the Red Sea, are also within range of Iran’s medium-range ballistic missiles.

Iran’s ballistic missile inventory has been aided by China, Russia, and North Korea. Iran possesses a family of liquid-fueled propellant missiles (the Shahab series) based on former Soviet Scud technology. The Shahab series, which can hit targets from 300 to 2,000 km away, constitutes the core of Iran’s missile force. Examples include the Shahab-1/-2/-3 variants like the Qiam-1, Ghadr-1, and Emad, which feature improved navigation and guidance components, lethality, and range.

Iran has also produced indigenously designed solid-propellant missiles (the Fateh series) with ranges of 200 to 2,000 km, based on Chinese technology. In addition, Iran possesses land-attack cruise missiles such as the Soumar and the Meshkat, with a range of approximately 2,500 km. Figure 1 illustrates the ranges of a sample of Iran’s missile inventory, including the Fateh-110 (300 km range), Zolfaghar (700 km), Shahab-3/Emad/Ghadr (2,000 km), and Soumar (2,500 km). It shows that Iranian missiles can reach all critical infrastructure in Saudi Arabia.

In addition to its own arsenal, Iran also relies on partners like the Houthis in Yemen. The Islamic Revolutionary Guard Corps-Quds Force, Iran’s primary irregular force, has provided weapons, technology, training, and advisers to the Houthis (officially called Ansar Allah). The Houthis have targeted ships near the Bab el-Mandeb Strait and conducted attacks against land-based targets in Saudi Arabia and the United Arab Emirates. The Bab el-Mandeb Strait, located at the southern end of the Red Sea between Yemen and Djibouti, is strategically important. Roughly 5 million barrels of oil pass through it every day, as does a substantial amount of global trade. Iran has provided the Houthis with weapons or technology for anti-tank guided missiles, sea mines, aerial drones (like the Qasef 2), 122-mm Katyusha rockets, Misagh-2 man-portable air defense systems (MANPADS), RDX high explosives, ballistic missiles like the Borkan-2H, and unmanned explosive boats.

The Houthis have used these systems to strike targets in Saudi Arabia on numerous occasions. In May 2019, for example, Houthis used several drones to target two pumping stations on Saudi Arabia’s East-West Pipeline, shutting it down for several days. The Houthis have also used Borkan-2H mobile, short-range ballistic missiles to strike Riyadh and other targets in Saudi Arabia. A United Nations panel of experts concluded that the missiles were “a derived lighter version” of Iran’s Qiam-1 missile and that Iran provided key missile parts to the Houthis. Analysis from the wreckage of 10 Borkan-2H missiles indicates that they were likely smuggled into Yemen in parts and then assembled. Iranian components were also integrated into Yemeni SA-2 surface-to-air missiles to construct the Qaher series of surface-to-surface rockets. Iran has likely used a number of routes to transport the material to Yemen, including ship-to-shore transfers through the Yemeni ports of Nishtun and Al-Ghaydah in Al-Mahrah governorate.

As Figure 2 highlights, we identified over 250 missile, unmanned aerial vehicle, and other attacks against critical infrastructure and other targets in Saudi Arabia over the past three years by the Iranian-linked Houthis. These numbers are likely low because there may be other attacks that are unreported in the press. Among the attacks we were able to confirm, the attacks have included direct fire, explosives (including from unmanned aerial vehicles), guided missiles, and indirect fire (including mortars, rockets, ballistic missiles, and unidentified projectiles). The vast majority of attacks were indirect fire (71 percent), and the most frequently targeted provinces in Saudi Arabia...
were Jazan (107 attacks), Najran (79 attacks), and Asir (39)—all near the Saudi Arabia-Yemen border.

Iran has also helped Lebanese Hezbollah improve its missile and other capabilities. Although Hezbollah will likely prioritize its precision weaponry for conflict with Israel, the group's missile arsenal and other capabilities could be utilized to attack Saudi Arabia or other targets. With Iran's help, Hezbollah has amassed a range of weapons and systems, such as the Fateh-110/M-600 short-range ballistic missile, Shahab-1 and Shahab-2 short-range ballistic missiles, Karrar unmanned combat aerial vehicles, and Katyusha rocket launchers. Hezbollah's armed drone capabilities are likely the most advanced of any terrorist group in the world. Hezbollah has provided training and other assistance to the Houthis, including to their drone and missile programs.

**CYBER CAPABILITIES**

Though missiles can directly target critical infrastructure in Saudi Arabia and the Persian Gulf, Iran will likely continue to engage in irregular attacks before escalating to direct conflict. One option is cyberattacks. Cyber tools offer virtually unlimited range and low attribution. Low attribution is especially attractive for the Iranians because it allows them to conduct sabotage and other operations while maintaining plausible deniability.

Iran has significantly improved its offensive cyber capabilities over the past several years. At least four organizations play a role in Iran's offensive cyber operations: the Islamic Revolutionary Guard Corps, Basij, Iran's Passive Defense Organization, and the Ministry of Intelligence and Security. As the U.S. Director of National Intelligence recently concluded, Iran "is capable of causing localized, temporary disruptive effects—such as disrupting a large company's corporate networks for days to weeks—similar to its data deletion attacks against dozens of Saudi governmental and private-sector networks in late 2016 and early 2017." Iran is also improving its ability to conduct more destructive and lasting cyberattacks. For example, many of Saudi Aramco's critical processes—such as drilling oil wells, pumping oil, and loading fuel onto tankers—are managed and monitored electronically. These systems can be targeted, even though Aramco has improved its cyber security defenses. The destructive malware Shamoon, which has been linked to Iran through the state-sponsored hacking group APT33 (or Elfin), involves a wiper malware (Trojan.Filerase) that deletes files from an infected computer and then wipes the computer's master boot record, making it unusable. Shamoon has been used to target oil and gas infrastructure in Saudi Arabia and the United Arab Emirates.

Moving forward, Iran will likely continue to use cyber operations as a major instrument against Saudi infrastructure in the Gulf, such as oil facilities. In the event of an escalation in hostilities, however, Iran also has the capability to target desalination facilities, the electrical grid, SCADA systems, and other critical infrastructure using offensive cyber operations.

**MARITIME ANTI-ACCESS/AREA DENIAL CAPABILITIES**

Iran employs a range of other irregular weapons and tactics to threaten critical infrastructure transiting strategic waterways like the Strait of Hormuz and the Bab el-Mandeb Strait. Tehran maintains a growing arsenal of mines, coastal defense cruise missiles, submarines, unmanned aerial vehicles, and fast-attack and patrol craft. For example, Iran possesses a large inventory of over 2,000 mines and has invested in new mines and mine-delivery vessels. Tehran has incorporated smaller vessels into its mine-laying strategy along with submarines and larger vessels.

Iranian mobile coastal-defense cruise missile launchers can readily be deployed along the Iranian coast, on Iranian-claimed islands in the Persian Gulf, and potentially even on oil platforms. Iran has expanded its inventory of coastal-defense cruise missiles from Chinese C802- and C700-series cruise missiles to domestically-produced variants, such as the Noor, Ghader, and Ghadir. The coastal-defense cruise missile threat is also extraterritorial. In 2006, Lebanese Hezbollah successfully used a C802 missile to target an Israeli naval vessel.

Iran is the only Persian Gulf country that possesses submarines, and the anti-sub capacity of regional countries is extremely limited. Iran's submarine force consists of three kilo-class submarines capable of laying mines and launching torpedoes, as well as other imported and domestically-produced midget-class submarines.

As part of its irregular naval doctrine, Iran employs smaller vessels that emphasize speed and mobility. Iran could employ these fast-attack vessels to fire on tankers, lay mines, or conduct swarming tactics to isolate and overwhelm targets. Iranian acquisition of the Houdong-class missile boats, C-14-class missile boats, and MK 13-class patrol craft (all from China) highlights Iran's focus on irregular capabilities and their ability to fire precision missiles from mobile maritime platforms. Iran also produces domestic variants, such as the Peykaap I-/II-class patrol craft and missile boats.

In short, Iran's swarming tactics and irregular capabilities suggest that it will continue to threaten critical infrastructure targets transiting through strategic waterways like the Strait of Hormuz and Bab el-Mandeb Strait.
VULNERABILITIES TO CRITICAL INFRASTRUCTURE

This section provides an overview of critical infrastructure vulnerabilities in Saudi Arabia that could be targeted in the event of escalating hostilities with Iran. While this section does not analyze specific conflict scenarios, it assumes that Iran would likely use missiles, drones, and cyberattacks in an attempt to neutralize command and control systems, air bases, and Saudi CSS-2 missile systems before attacks on infrastructure. In addition, this analysis is not intended to be comprehensive, but rather to highlight four systems that pose opportunities for Iranian aggression or retaliatory measures. These include oil production and export infrastructure, desalination plants, the electricity grid, and supervisory control and data acquisition (SCADA) systems.

OIL INFRASTRUCTURE

Saudi Aramco has devoted considerable resources to protecting its infrastructure from missile, cyber, and other attacks. Still, the threat to Saudi Arabia’s oil infrastructure remains significant. Iran or one of its partners could attack the upstream components of Saudi Arabia’s oil infrastructure, which includes exploration and production of its oil fields. Such an attack might temporarily impact global oil markets, but it would likely have little affect on Saudi Arabia’s oil infrastructure. Saudi Arabia operates one of the world’s largest onshore oil fields, Ghawar, and the largest offshore field, Safaniyah, which together hold approximately 110 billion barrels of proven oil reserves. Production on these and other Saudi fields involves numerous wells spread across vast areas of land, making target selection difficult and the likelihood of significant damage low. Ghawar, for example, covers 2,600 square miles.

Oil is pumped from the fields to gas-oil separation plants (GOSPs) to remove non-oil elements before processing. There are more than 60 GOSPs across the country. Each has a relatively small capacity in proportion to Saudi Arabia’s total production, which would make it difficult for Iran to cause significant damage.

From GOSPs, however, the majority of Saudi oil is moved to stabilization plants, which offer a potentially more vulnerable target in the event of escalating hostilities. Saudi oil is mostly “sour,” which means that it contains significant amounts of hydrogen sulfide that must be removed prior to shipping.

This process occurs at several stabilization facilities located...
across Saudi Arabia, including at Abqaiq, Jubail, Qatif, and Ras Tanura. Of these, Abqaiq is the most vulnerable. It is the world’s largest oil processing facility and crude oil stabilization plant, with a capacity of more than 7 million barrels per day (bpd). Though the Abqaiq facility is large, the stabilization process is concentrated in specific areas highlighted in Figure 3—including storage tanks and processing and compressor trains—which greatly increases the likelihood of a strike successfully disrupting or destroying its operations.

Following stabilization, crude oil is either pumped to a port for exporting or to a refinery for processing into commercial products, including gasoline and diesel fuel. Saudi Arabia currently has nine refineries in operation, with the largest located in Ras Tanura, Jubail, Rabigh, and Yanbu. One additional refinery—in Jazan, located in southwestern Saudi Arabia near its border with Yemen—is scheduled to be operational by the end of 2019. Refined product exports help fuel Saudi Arabia’s economy, though they are smaller in volume than crude oil exports. Of Saudi Arabia’s exports, 7.4 million bpd are crude oil, while only around 1.9 million bpd are refined products.

Saudi Arabia’s export mechanisms are also potentially vulnerable, including its system of pipelines and its ports along the Persian Gulf and Red Sea. Its primary domestic pipeline is the 746-mile Petroline (also known as the East-West Pipeline), which connects processing facilities in eastern Saudi Arabia to export facilities along the Red Sea like Yanbu, thus allowing crude oil exports to bypass the Strait of Hormuz. The Petroline's capacity is currently 5 million bpd, but expansion is currently underway to significantly increase that capacity over the next several years. To move oil to Red Sea ports, which are located at a higher elevation than eastern processing facilities, the Petroline operates using a series of pumping stations. An attack on any of these pumping stations could halt the flow of oil in that direction. But Saudi Aramco has established safety measures to mitigate damage and rapidly restore pipeline function in the event of an attack. These measures include monitoring systems to quickly identify damage, shutoff valves within the pipeline to limit oil losses, and pre-positioned replacement parts around the country to expedite repairs.

In addition, attacks on Saudi ports, especially those along the Gulf, could inflict significant damage. Ras Tanura, located on the Gulf, is both Saudi Arabia’s primary port and the world’s

Figure 4: Ras Tanura Oil Terminal – Main
largest offshore oil exporting port. Its components, depicted in Figures 4 and 5, consist of a large storage facility; two attached loading terminals for use by small crude carriers, which are connected by above-water supply pipelines to the main storage facility; and an offshore loading terminal for use by Very Large Crude Carriers (VLCCs), which is connected to the storage facility by multiple buried pipelines. Ras Tanura has an average handling capacity of 3.4 million bpd and loads all Saudi crude oil grades. The port of Ras al-Juaymah, to the north, has an average handling capacity of 3 million bpd. Together, these two Gulf ports handle nearly 70 percent of Saudi Arabia’s oil exports.

Yanbu, located on the Red Sea, is Saudi Arabia’s third-largest oil export facility. Its average handling capacity is 1.3 million bpd—less than half the capacity of either Ras Tanura or Ras al-Juaymah—and it currently only handles shipments of the Arab Light crude oil grade. However, up to 5 million bpd could be diverted to Yanbu and other smaller Red Sea terminals (such as Jeddah, Jazan, Rabigh, and the recently reopened Muajjiz) via the Petroline in the event of an attack, making Yanbu a potential secondary target.

**DESALINATION FACILITIES**

Natural renewable water resources are scarce in Saudi Arabia, Kuwait, Qatar, Oman, and the United Arab Emirates. Limited rainfall and excessive consumption have depleted groundwater to unsustainable levels. As a result, water desalination is vital to acquiring potable water. Gulf Cooperation Council countries host 43 percent of the world’s total desalination plants (7,500 of 17,500) and account for about 70 percent of the global total production capacity for desalinated water. In Saudi Arabia, desalination accounts for over 70 percent of the potable water used in cities, and desalinated water has replaced groundwater as the primary source of drinking water throughout the country.

The world’s largest desalination plant is Ras al-Khair, located on the Persian Gulf coast of Saudi Arabia just north of Jubail. The plant was commissioned in 2014 and has a daily production capacity of 1.025 million cubic meters of desalinated water. The majority of the water produced (some 800 cubic meters per day) goes directly to Riyadh, while the other 200 cubic meters is distributed to
neighboring regions. Ras al-Khair is a hybrid plant, which uses multistage flashing and reverse osmosis technologies to remove salt from the water pumped in from the Gulf. The eight multistage flashing units heat the seawater to produce steam, then condense the steam to form desalinated water, while the seventeen reverse osmosis units force seawater through semi-permeable membranes to remove the sodium and chloride. The multistage flashing units and other components of the desalination process are highlighted in Figure 6.

In 2009, leaked U.S. State Department diplomatic cables suggested that a hostile act against Saudi Arabia’s desalination plant at Jubail would force Riyadh to evacuate “within a week,” as the plant at that time provided Riyadh with over 90 percent of its drinking water. Ras al-Khair is now Saudi Arabia’s (and the world’s) largest desalination plant and is also vulnerable to an Iranian attack. In one assessment, analysts noted that “every desalination plant built is a hostage to fortune; they are easily sabotaged; they can be attacked from the air or by shelling from off-shore; and their intake ports have to be kept clear, giving another simple way of preventing their operation.” Cyberattacks also present a serious threat to Saudi desalination plants like Ras al-Khair. Beyond these types of attacks, Saudi Arabia and its neighbors need to worry about the water quality itself. An intentional (or even an unintentional) oil spillage near Ras al-Khair, for example, would render the water unusable for desalination, a concern which was realized during the Gulf War after Iraq deliberately opened the valves at a Kuwaiti oil terminal and created a massive oil slick in the Gulf.

While facilities like Ras al-Khair are vulnerable to an attack, Iran has not significantly targeted desalination plants in the past. This may be because attacking a strategic desalination plant would be a hostile act of war and signify a major escalation in conflict. It might also be because it is a civilian—rather than a military or commercial—target with significant humanitarian ramifications. Still, it is possible that Iran or one of its partners like the Houthis could target a component of the desalination system—such as water pipelines—which causes limited damage but signals Iran’s ability to escalate further.

Figure 6: Ras al-Khair Desalination Plant
ELECTRICAL GRID

Saudi Arabia’s rapidly expanding population and industrial infrastructure has also increased its electricity demand, with domestic consumption rising at a rate of 7 percent through 2017. Its electrical supply has struggled to keep up with this demand, as many segments of its current grid—including substations and transformers—are outdated and inefficient. The combination of increased load and inefficient infrastructure has led to shortages, including brownouts and blackouts, in various parts of the country over the past several years.

Beyond the problems caused by the infrastructure itself, Saudi Arabia’s electrical grid offers at least four potential vulnerabilities in the event of an Iranian attack. First, a successful attack on the oil and gas sector could also impact the electrical grid. Due to its significant oil reserves and heavily subsidized domestic oil prices, Saudi Arabia is largely dependent on hydrocarbons as fuel for the electricity sector. Crude oil is used as the input in nearly two-thirds of electricity generation, and natural gas serves as fuel for most of the remaining portion. Second, transformers serve as the link between generators and transmission stations, as well as between transmission and distribution systems, and are relatively easy to target using explosive attacks. Third, most electrical power systems are constantly monitored and adjusted by SCADA systems—explored in more depth in the following section—and can be disrupted by cyberattacks. Fourth, a coordinated attack on multiple transmission lines or substations could overload generators and create a cascading transmission failure, potentially leading to widespread blackouts. This last scenario is unlikely because of its low probability of success. Attackers would need to know which substations and transmission lines to attack—and target them simultaneously. But the potential impact could be significant.

SCADA SYSTEMS

Industrial control systems (ICSs) and supervisory control and data acquisition (SCADA) systems also present a serious vulnerability. SCADA systems are the industrial control interfaces that help regulate large-scale infrastructure like gas pipelines, power transmission systems, transportation systems, and water distribution systems. They monitor inputs from automated processes and give operators the ability to observe and manipulate those processes in real time, either by creating an alert in instances of irregularity or by automatically adjusting the process to return to normal when an irregularity occurs.

A SCADA network, such as those used in the systems mentioned above, consists of the following components:

- Sensors (either digital or analog) and control relays, which directly interface with the managed system;
- Remote telemetry units (RTUs), which are generally small, hardened computerized units deployed in the field to serve as data collection points;
- Master units, which are larger computer consoles that serve as the central processor for the SCADA system and as the hub of human-machine interface; and
- A communications network, which connects the master unit to the RTUs in the field.

All of these components may be vulnerable to attack by direct human interference (such as the deployment of malware in the master unit) or by poor design or configuration, which opens up the system to remote cyber exploitation.

Broadly, a SCADA attack seeks to manipulate the functioning of the system in order to interrupt normal functioning or to damage the physical infrastructure of the system it attacks. Two examples highlight the possibility to create physical damage. The first was the U.S.-Israeli Stuxnet attack against Iran, or Operation Olympic Games, which targeted Siemens SCADA systems in order to sabotage centrifuges used for uranium enrichment. The second was a lesser-known attack in 2014 against a German steel mill, where hackers prevented the shutdown of a blast furnace and caused substantial damage.

Since 2012, Saudi SCADA systems have been attacked on several occasions. On August 15, 2012, Saudi Aramco was hit by the Iranian-linked malware Shamoon, which stole—and then overwrote—data on over 30,000 Aramco computers, rendering them unusable. Shamoon may have been designed by Iran as a retaliation for a similar SCADA attack on its oil infrastructure that had been discovered months previously, as well as the Stuxnet attack in 2010. In November 2016, Iran-linked hackers launched Shamoon again, this time against Saudi Arabia’s General Authority of Civil Aviation and at least five other agencies. Operations were brought to a halt for several days, and thousands of computers had critical data erased. In January 2017, computers at the National Industrialization Company and Sadara Chemical Company had their data wiped and hard drives destroyed. And in August 2017, a malware attack with a virus known as “Triton” or “Trisis” attempted to sabotage physical operations of a Saudi petrochemical plant, but a misconfiguration caused the affected machines to shut down instead of exploding. Previous cyber attacks on...
Aramco’s information and computer systems caused back-ups at Ras Tanura in loading oil onto tankers, and forced operators to resort to faxing information on tanker loadings. Cyberattacks against Saudi ICSs and SCADA systems present a significant threat, though Iranian attacks thus far have been limited in their scope and damage. In addition, Saudi Arabia’s cyber defenses have improved in recent years.

**DETERRING IRANIAN ACTIONS**

Despite the increase in U.S.-Iranian tensions, Tehran has adopted a calibrated approach to targeting critical infrastructure in Saudi Arabia and other Gulf countries. It has focused on irregular strategies and tactics—such as conducting cyber operations, harassing tankers, and supporting attacks from partner forces like the Houthis—rather than using significant direct force. Iran almost certainly wants to limit military escalation and prevent interstate war. Still, it is possible that Iran, the United States, or other countries could escalate the current conflict through miscalculation or even deliberate actions. Consequently, the United States should consider several steps to prevent escalation and protect critical infrastructure in countries like Saudi Arabia.

First, the U.S. government and private sector should continue to help Saudi Arabia and other regional countries harden their critical infrastructure from Iranian strikes. In response to Iranian or partner cyber operations, examples might include continuing to improve the integrity, resiliency, and redundancy of cyber networks. In response to Iranian or partner missile or drone strikes, the United States should continue to support the development of a complex network of bases and command centers that are hardened against possible strikes, well-dispersed, and situated beyond the range of Iran’s most numerous attack systems. Military planners should also ensure that sufficient stocks of air-delivered munitions are stored in survivable ways in the region.

To detect and protect against Iranian and partner attacks, the United States should ensure that it keeps sufficient numbers and types of mine countermeasure vessels; land-based fighter aircraft; Patriot and Terminal High Altitude Area Defense (THAAD) surface-to-air missile batteries; high-end intelligence, surveillance, and reconnaissance (ISR) orbits; and attack submarines. There have been numerous debates within the Trump administration (like the Obama administration) about shifting U.S. military resources away from the Middle East to Asia and Europe in order to balance against China and Russia. But based on the heightened tensions between the United States and Iran, it would be a mistake to decrease the current U.S. military posture in the Middle East. Saudi Arabia also needs additional missile capabilities and seeks systems like the Dongfeng 5 ballistic missile from China if the United States and its partners are unwilling to help.

Second, the United States and its partners should focus on deterring Iranian escalation through the threat—and when appropriate—the use of measured offensive actions. As Thomas Schelling argued in his influential study *Arms and Influence*, “it is the threat of damage, or of more damage to come, that can make someone yield or comply. It is latent violence that can influence someone’s choice—violence that can still be withheld or inflicted, or that a victim believes can be withheld or inflicted.” The United States needs to continue to communicate to Iran that major attacks against Saudi and other critical infrastructure—which do significant damage to oil and gas infrastructure, desalination facilities, electricity grids, SCADA systems, or other infrastructure—will be met with a harsh response. Deterring Iran requires signaling the intent and capabilities to strike Iranian targets, including by continuing to have a robust U.S. second-strike capability.

The challenge, however, is that it will be difficult—and perhaps impossible—to deter Iran from some types of offensive cyber operations and irregular attacks from partners, such as the Houthis. This is the nature of irregular warfare. The U.S. diplomat George Kennan referred to this type of routine warfare as “the perpetual rhythm of struggle” between states. Consequently, the United States should focus on deterring escalatory missile and cyberattacks against oil, desalination, electricity, SCADA, and other infrastructure.

A proportionate U.S. response to Iranian aggression will depend on the specific scenario. But the United States should generally aim to respond in ways that don’t escalate the conflict. In addition, the United States does not always need to respond directly to Iranian activity, but can operate by, with, and through partners in the region. Examples of actions in response to Iranian hostility might include targeting unmanned Iranian drones; seizing Iranian ships, including tankers; targeting Iranian partner forces in countries like Yemen and Syria; and conducting measured offensive cyber operations against Iranian air defense, military command and control, or critical infrastructure systems. Any U.S. or partner action should be accompanied by clear messages to Iran’s leadership about further
responses—what Schelling referred to as the threat of latent violence—if Iran continues to act aggressively.

Third, the United States should be careful not to threaten the survival of the Iranian regime, which would raise the prospects of escalation and interstate conflict. President Trump publicly noted that “we’re not looking for regime change” in Iran, which is a helpful step. But it is less clear whether this sentiment is shared by other senior U.S. officials. Over the past two decades, the U.S. overthrow of regimes in Afghanistan (2001), Iraq (2003), and Libya (2011) triggered destabilizing wars and regional turbulence. Some U.S. policymakers may hope that economic sanctions will trigger a groundswell of resentment against the Iranian government that eventually leads to regime change. But regime change through sanctions is unlikely to occur, and there is little evidence that the Iranian government is in danger of collapsing.

One challenge with the current U.S. approach is that it is too reliant on economic sanctions, which may severely weaken Iran’s economy but are unlikely to dissuade Iran from developing its missile program or aiding partner forces in countries like Syria, Iraq, Yemen, and Lebanon. In fact, escalating sanctions—without clear and achievable U.S. political objectives—will likely increase Iran’s efforts to strengthen these capabilities. The United States needs to clearly signal to Tehran a way out of the current conflict. Iran is unlikely to give up its missile program. But it may eventually agree to a nuclear deal in exchange for sanctions relief, which it already agreed to under the Joint Comprehensive Plan of Action (JCPOA). In addition, Tehran will not end its support to partner forces like Lebanese Hezbollah in the region, but it may be willing to help seek a political solution to the Yemen conflict and curb its support to the Houthis.

In the end, U.S. policymakers would be wise to heed Schelling’s advice on latent violence. The best way to protect critical infrastructure in countries like Saudi Arabia may be to develop a robust deterrent strategy that credibly signals to Iran—through words and actions—that it will be punished if it moves up the escalatory ladder, as well as offers a political exit ramp to the current conflict.

Seth G. Jones is the Harold Brown Chair and director of the Transnational Threats Project at the Center for Strategic and International Studies (CSIS). Danika Newlee is a program manager and research associate for the Transnational Threats Project at CSIS. Nicholas Harrington is a research assistant and program coordinator for the Transnational Threats Project and the Arleigh A. Burke Chair in Strategy at CSIS. Joseph S. Bermudez Jr. is a senior fellow for Imagery Analysis at CSIS.

The authors give special thanks to several anonymous reviewers for their comments on the document, as well as Alex Friedland for his assistance in collecting and analyzing data.

This brief is made possible by general support to CSIS. No direct sponsorship contributed to this brief.


11 Ibid.


14 Coats, World Threat Assessment of the U.S. Intelligence Community, 30.


18 Knights, “The Houthi War Machine.”


20 Knights, “The Houthi War Machine.”


26 Coats, World Wide Threat Assessment of the U.S. Intelligence Community, 6.

27 Lewis, “Iran and Cyber Power.”


31 ONI, Iranian Naval Forces: A Tale of Two Navies.

32 ONI, Iran’s Naval Forces: From Guerilla Warfare to a Modern Naval Strategy.


34 ONI, Iran’s Naval Forces: From Guerilla Warfare to a Modern Naval Strategy.


37 ONI, Iran’s Naval Forces: From Guerilla Warfare to a Modern Naval Strategy.

38 Ibid.

international/analysis_includes/countries_long/Saudi_Arabia/saudi_arabia.pdf.
41 Ibid.
42 EIA, “Country Analysis Brief: Saudi Arabia.”
44 EIA, “Country Analysis Brief: Saudi Arabia.”
45 Ibid.
48 EIA, “Country Analysis Brief: Saudi Arabia.”
50 Shifrinson and Pribe, “A Crude Threat.”
51 EIA, “Country Analysis Brief: Saudi Arabia.”
56 DeNicola, “Climate Change and Water Scarcity.”
65 Ibid.
66 See, for example, DPS Telecom, “What is SCADA?” https://www.dpstele.com/scada/what-is.php.
67 Ibid.
75 Thomas C. Schelling, Arms and Influence (New Haven, CT: Yale University Press, 2008), 3. The italicized words are in the original text.