

The Postwar Threat to Gulf Energy Infrastructure

OCTOBER 2026

By Daniel Byman
and Alden Ness

In the U.S. and Israeli war against Iran, Tehran's strongest weapon has been its ability to threaten oil and gas shipping through the Strait of Hormuz. This threat devastated regional energy exporters: A month into the war, Saudi Arabia's oil exports had fallen by **more than a third**, those of the United Arab Emirates (UAE) were reduced by over **50 percent**, and Kuwait's and Iraq's **had ceased almost completely**. Within the same time frame, Qatar's and the UAE's liquefied natural gas (LNG) exports were entirely **cut off**. In addition to successful **attacks** on oil and LNG tankers, the very threat of such strikes led to a decline in commercial shipping: In the early months of the war, shipping companies were hesitant to **endanger** their personnel, and insurance companies **refused** to provide insurance or charged much higher rates. Although shipping increased over time, concerns about risk remained high.

As the on-again, off-again conflict continues, Iraq and the Gulf states are adapting. Saudi Arabia and the UAE have **used pipelines** to export some oil and thus partially avoid Iran's cutoff of traffic. Now, there are at least seven new or expanded major pipeline projects designed to bypass the Strait of Hormuz, sending oil to the Red Sea, the Gulf of Oman, or the Mediterranean Sea to be shipped from there. Goldman Sachs **estimates** that these projects could add almost 4 million barrels of export capacity per day by the end of 2027 and over 7 million by the end of 2028. Once complete, such projects would **reduce** the importance of the Strait of Hormuz and thus Iran's coercive leverage, although Iran has already shown its ability to target the flow of oil in other parts of the region, both directly and via proxies. In addition, oil exporters have **altered** ship-to-ship operations and other forms of energy supply transfer, accepting risk in order to facilitate the movement of oil. National oil companies are also

self-insuring, and some suppliers are **relying on the United States** government for insurance, **buying their own tankers**, and otherwise taking on more risk.

From a security point of view, these new pipelines and other forms of adaptation have many advantages. They will operate farther from Iran than shipping traffic in the Gulf, which Iran can strike with relative ease. Pipelines are vulnerable neither to dramatic spikes in the cost of shipping insurance nor to the safety concerns of human crews. Multiple pipelines are particularly valuable, as they increase the number of options for export, making total supply disruption difficult. The pipelines are expensive, however, with total **costs** to the Gulf states for repairing and improving pipelines, refineries, and other infrastructure in the tens of billions or more.

Iran will want to have the ability to disrupt the flow of oil and gas in case of a future conflict and to coerce regional states on issues including ties to Israel and disputes elsewhere in the Middle East.

Tehran, meanwhile, is not likely to stand by as the Gulf states seek to reduce its leverage. Iran will want to have the ability to disrupt the flow of oil and gas in case of a future conflict and to coerce regional states on issues including ties to Israel and disputes elsewhere in the Middle East (such as in Lebanon and Yemen). Iran will also want to wield the threat of disruption over regional exporters to gain more sanctions relief and other economic rewards, both in the immediate conflict and in the future. Indeed, Iran is already adapting: In July 2026, Iranian-backed Houthi rebels in Yemen began **targeting** Saudi tankers in the Bab el-Mandab, threatening another supply route.

Although pipelines offer security advantages when compared with shipping through the strait, the pipelines—and the region’s oil infrastructure in general—remain vulnerable to Iranian attacks. Iran and Iranian-backed groups can use explosive devices to sabotage pipelines, launch unmanned aerial vehicle (UAV) and missile attacks on critical nodes such as separation facilities and pumping stations, conduct cyberattacks, and otherwise threaten regional energy infrastructure. If such attacks occurred on a large scale, they could reduce the global supply of oil and gas.

Any Iranian disruptions, however, will probably be episodic and incomplete. Gulf exporters will absorb some disruptions as a cost of doing business, and there may be a back-and-forth in which Iran uses sabotage and limited attacks to disrupt production while exporters defend and repair pipelines and other infrastructure. Moreover, not all Gulf states are equally vulnerable. Some have better security services and more resources to devote to defense, while others—notably Iraq—have a large number of pro-Iran militants that Tehran can call upon should it

choose to do so. In addition, Iran sees some regional states as particular enemies while others—again, notably Iraq—are often de facto partners.

The remainder of this paper has four parts. First, it discusses the range of potential targets that Iran might strike and the means it might use to do so. (The paper does not go into detail on the risks of cyberattacks, an important topic that merits its own in-depth treatment.) The second section describes which Iranian threats are relevant to Iraq, Saudi Arabia, the UAE, and other regional states. The third section examines the implications of Iranian attacks on oil and gas infrastructure. The final section assesses implications for the United States and its allies.

Potential Threats to Oil and Gas Infrastructure

The oil and natural gas extraction, processing, transport, refining, and storage process relies on a highly interdependent network of infrastructure. The industry traditionally designates segments of this network into broad categories of “upstream,” “midstream,” and “downstream,” based on ordering and function in the overall process. These designations are important to understanding how energy moves from field to market and what security challenges arise in each part of the network.

Upstream infrastructure is responsible for extraction directly from oil and gas fields, as well as initial processing of obtained output. It includes wellheads that pump pressurized crude and gas from individual wells into gathering pipelines and manifold systems, which collect and distribute the flow of oil among multiple destinations. Gas-oil separation tanks [handle](#) basic processing of material, which is metered at custody transfer points and blended with the output of multiple wells. The resulting mixtures are then transported to midstream facilities.

Midstream infrastructure is responsible for transporting product to final-step facilities before it can be consumed. Pipelines feed partially processed oil and gas into large processing facilities for treatment into forms that are transportable en masse. Product pipelines then route this treated oil and gas to various places: export terminals where it is loaded onto tankers, domestic sites for local consumption, or export pipelines that flow to other countries overland and underwater.

Downstream infrastructure is responsible for the final processing of oil and gas into forms that are readily usable for the consumer and for delivery of product to market. This includes refineries that distill oil into various grades such as diesel and jet fuel, as well as petrochemical plants that convert hydrocarbons into plastics and rubbers. Downstream infrastructure also includes various market distribution mechanisms such as gas stations.

All aspects of the above-outlined network are deeply interdependent. The output from wellheads upstream must flow rapidly through pipelines, be processed quickly at midstream facilities, and be exported soon after. A disruption along any link in this chain reduces the network flow—and, if not addressed quickly, forces the entire network to compensate by reducing production levels.

In the Gulf countries, state-owned, vertically integrated national oil and gas companies dominate the oil and gas sectors. This means that all upstream, midstream, and downstream infrastructure is **managed** by one corporate entity that is mostly nationally owned. Accordingly, Gulf countries' oil and gas infrastructure is characterized by centralized planning within each country and little integration among countries.

Oil and gas infrastructure in the Gulf is dominated by state-specific network consolidation. Vertically integrated companies route most of the processing through large facilities across all segments of the production network. In upstream Gulf country operations, individual gathering facilities and central processing facilities (CPFs) often conduct initial treatment of millions of barrels per day (bpd). Midstream operations in the region depend on processing mega-centers and high-capacity pipelines and export terminals. Downstream operations are usually limited to a small number of large refineries.

Because select individual sites for oil and gas infrastructure are high capacity, an attack on any one facility can have a disproportionate impact on the entire network. This was demonstrated in 2019 when a Houthi attack on the Abqaiq mega-plant in Saudi Arabia brought over 5 million bpd offline for approximately three weeks, **resulting** in a temporary 5 percent reduction in global energy supply. Aramco did an impressive job **making repairs**, but future attacks may cause more lasting damage.

Network consolidation, while offering potential economies of scale regarding transport and export capacity, also involves trade-offs in the capacity to flexibly respond to a disruption from an attack. It is difficult for Gulf countries to reroute oil and gas to other states because their systems are so centralized and lack integrated infrastructure. When an attack limiting processing or export capacity takes place, extracted product is often trapped in a singular network with no way out.

In a postwar landscape, Iran may disrupt infrastructure that diffuses network capacity within or among countries, because this diffusion represents a threat to Tehran's leverage. This includes the **proposed** pipeline projects that would link Gulf countries to alternative export routes. Iran may also aim to disrupt the smooth function of existing consolidated oil and gas networks in the Gulf.

As discussed in the following subsections, Iran has two kinetic means to disrupt oil and gas infrastructure. First, Iran could conduct aerial attacks, including missile and UAV strikes. Second, Iran could perform ground and sea sabotage using covert networks that employ close-range weapons such as improvised explosive devices (IEDs).

Missile and UAV Threats

The proliferation of drones has increased the vulnerability of Gulf oil and gas facilities. Houthi strikes on the Abqaiq facility in 2019, coordinated with Iranian assistance, first demonstrated the **effectiveness of drones** in causing mass disruptions to Gulf infrastructure.

The proliferation of drones has increased the vulnerability of Gulf oil and gas facilities.

Riyadh ramped up security to **protect** against future attacks—increasing radar and air defense systems, among other things—but more recent attacks have proven those protection efforts to be insufficient. During the 2026 war, Iranian-backed Iraqi Shia militias targeted the Abqaiq facility using UAVs. Yet again, the **attacks** brought production capacity temporarily offline. They occurred in coordination with devastating Iranian **strikes** on Qatari and Kuwaiti facilities and successful Houthi **strikes** on Saudi oil and gas facilities lining the Red Sea. According to one Armed Conflict Location & Event Data analysis, over **70 percent** of strikes on critical infrastructure that penetrated air defenses resulted in **damages** during the 2026 war, through August of that year.

Next-generation Iranian UAV production allows for **cheap**, extended-range munitions that can overwhelm expensive and imperfect air defense systems, although **both Iran and its adversaries** are improving on offense and defense. From western Iran, northern Yemen, or southern Iraq, Iranian-linked actors can reach almost all the territory of the Gulf States using Iranian-produced UAVs such as the Samad-3, which the Houthis employ. The cost of these drones **begins** at approximately \$10,000 per unit. They can loiter and conduct reconnaissance before striking, and swarms of them can overwhelm the defense systems that are currently deployed. These new UAV threats augment to other types of UAVs and substantial missile capabilities that can **target** most Gulf countries.

Postwar missile and UAV targeting will probably continue to threaten upstream, midstream, and downstream infrastructure. Attacks will likely involve a combination of mass strikes on critical nodes in oil and gas networks and targeted strikes on remotely located infrastructure.

Onshore wellheads, gathering and manifold systems, and separation tanks process and move oil and gas in relatively small batches during and immediately following extraction. The cost of launching drones or missiles at these targets would generally not make sense given their lesser worth; as a result, past sabotage operations in the Middle East typically have not targeted this infrastructure, although cost declines in UAVs may change this calculation. An important exception, however, involves upstream facilities that are jointly managed by Western companies that Iran and its proxies **perceive** as enemies.

Some high-capacity upstream targets are at risk of aerial attacks. Offshore rigs, which often produce at a large scale, are more difficult to repair than their onshore counterparts. They can be **attacked** using drones and naval missiles and have been targeted during the war. CPFs are centralized sites for upstream processing of raw product from many wellheads and can be located either onshore or offshore. UAV or missile attacks on CPFs could halt production of massive oil and gas fields; as an example, CPFs in Saudi Arabia were targeted in April 2026 UAV strikes, with Khurais and Manifa fields halting production and **cutting output** by a combined 600,000 bpd. Similarly, onshore wellheads and gathering and manifold systems that maintain flows from larger fields are possible targets.

Unlike upstream operations, midstream operations are vulnerable to aerial attack because they involve infrastructure nodes that are critical to maintaining network flow. Midstream mega-facilities, for example, are responsible for processing the output of wells—averaging in the millions of bpd of oil—so that it is ready for transport. When these facilities are damaged, the entire system of production must slow or be rerouted until repair is complete. Additionally, storage tanks are likely targets that play an important role in relieving network overflow by holding spare inventory that often numbers in the **tens of millions** of barrels.

Iran and its proxies are likely to launch aerial attacks on pipelines that transport products between facilities. These routes are under continuous threat, as the 2026 Houthi UAV **attacks** on the Saudi East-West pipeline demonstrated. Because internal pipelines typically stretch over long distances, they are difficult to defend by air. Pipeline pumping stations, located along the length of the line to maintain proper pressure, are also prime targets.

Iran and its proxies are likely to launch aerial attacks on pipelines that transport products between facilities. These routes are under continuous threat, as the 2026 Houthi UAV attacks on the Saudi East-West pipeline demonstrated.

Above all, the infrastructure most vulnerable to Iranian-linked aerial attacks are systems related to midstream export operations. During the war, dozens of tankers became primary targets for missiles and drones aiming to slow shipping

in the Strait of Hormuz. After the war, tankers in the Strait of Hormuz or in the Bab-al-Mandeb will continue to be **threatened** by the same weapons. Export terminals—highly centralized facilities that are required to load large amounts of oil and gas onto tankers—have been attacked during the war and remain potential targets. Export pipelines pose the same aerial security challenges as internal pipelines do; they are difficult to defend and have vulnerable pumping stations.

The damages from aerial attacks on midstream infrastructure often extend beyond the network level to disrupt the wider environment. Attacks on tankers—for example, the June 2026 **attack** on the *Caroline Bezege* off the coast of Oman—can cause oil spills that disrupt marine life, fishing, and tourism. Similar damages may occur following attacks on offshore processing, transfer, and rig setups, onshore pipelines, and large processing facilities. Catastrophic spillage is especially likely if these facilities are located near large populations or water sources.

Lastly, certain downstream systems such as refineries and petroleum plants are susceptible to UAV and missile attacks. The Houthis attacked refineries during the 2026 war, including facilities in **Saudi Arabia**, Kuwait, and **Bahrain**.

Covert Ground and Sea Sabotage

The long history of ground and sea sabotage of oil and gas infrastructure allows for the mapping of possible future trends. **According** to University of Maryland's Global Terrorism Database, the most common sabotage on oil and gas has come in the form of IED attacks, rocket and mortar attacks, attacks on oil and gas workers, and coordinated ground captures. Iranian sabotage of Gulf infrastructure will likely use these methods.

Upstream, there are few examples of successful wellhead attacks in areas where a government controls territory. Highly disruptive wellhead targeting requires many explosives and a coordinated system to plant and detonate across sites. Even insurgents who might exploit weak government control rarely have had the means for such an attack. Groups that are funded and directed by Iran are better able to engage in wellhead sabotage, which can inflict damage after just a single night of planting explosives. Even that, however, may prove difficult for many groups, and they are likely to prefer to use their resources for other attacks.

Aside from wellheads, upstream infrastructure systems—including preliminary onshore treating systems such as manifold pipelines, gathering pipelines, and gas-oil separation plants—are vulnerable. Some of this early-stage treatment infrastructure is small-scale and located close to wellhead sources, making it vulnerable to ground attack because it is not as closely guarded.

Upstream offshore infrastructure is also vulnerable, especially to aerial attack. Offshore rigs and processing centers typically handle large flows, making them attractive targets that are relatively ungarded. Attacks using planted explosives are difficult; the Iran-Iraq War, for instance, saw **disastrous** attempts to disable offshore rigs. Later attacks offshore have involved isolated incidents by the U.S. military and occasional inconsequential Iranian forays.

Midstream operations are more likely to be attacked covertly. Internal pipelines can be targeted by nonstate actors using IEDs and close-range rocket propelled grenades, a tactic **employed** by various Iraqi insurgent groups. Some internal pipelines are linked to individual multinational companies that Iran may wish to sabotage, raising their risk profile; **attacks** on U.S.-linked pipelines in Nigeria are an example of this directed strategy of attack.

Export pipelines are similarly vulnerable to targeting by Iran. The only currently operating export pipeline in the Middle East—the Kirkuk-Ceyhan pipeline—has been **targeted** dozens of times by nonstate groups using IEDs and missile and mortar launches. Ground-based attacks on export pipelines often involve explosives planted opportunistically along the length of the line, without regard for critical nodes.

More generally, attacks on upstream and midstream infrastructure have sometimes involved pirating, hostage taking, and assaults on crews. Offshore rigs and terminals are **ideal** for hostage takers because of the difficulties that authorities face in reaching them and the cramped nature of their spaces, which have few entry points. Attacks on pipeline crews are rare but can be devastating. A 2014 **militant attack** on the Kirkuk-Ceyhan line was followed by an entrenchment of the militants' position in Iraqi Kurdistan. The militants chased off **repair crews** and prevented recovery for months.

Newly constructed export pipelines and existing internal pipelines will likely face the same or similar on-the-ground threats. Ground-based pipeline attacks are especially difficult to detect and defend against because lines often run through hundreds of miles of remote territory; a majority of recorded pipeline attacks remain **unattributed** to this day. A major threat involves Iran's support of insurgent groups and lone actors operating in or near countries that maintain export pipelines.

Lastly, the ground-level sabotage of downstream infrastructure is uncommon in Gulf countries, because these facilities are usually well-guarded.

Future Threats to Key Countries

The threat to regional oil exporters varies considerably by country and depends on both the countries' individual vulnerabilities and the degree of Iran's hostility toward each.

Iraq

Iraq is probably the country most vulnerable to attacks on its oil and gas infrastructure, though Iran may hesitate to strike it. Iraq's economy is highly dependent on oil and features concentrated and aging export infrastructure, weak state control, and the presence of numerous autonomous armed groups. Despite these vulnerabilities, Iran has stronger strategic reasons to avoid attacking Iraqi state infrastructure in comparison with the Gulf states.

Iraq is probably the country most vulnerable to attacks on its oil and gas infrastructure, though Iran may hesitate to strike it.

Iraq suffers considerable political violence, and Iran exerts tremendous influence in the country. Iran has numerous and close ties to political leaders in Iraq at both the national and local levels, as well as ties to armed groups and religious institutions. As a result, Iran has a deep intelligence network in Iraq and the ability to shape (but not control) government policy. Tehran also has access to different militia groups, such as Kataib Hezbollah and Asaib Ahl al-Haq, that probably would attack Iraqi pipelines if Tehran ordered them to. Iran **does not** exercise complete control of these groups, but it does have considerable influence.

Baghdad, however, also works closely with Tehran at times, and in general is not hostile or seen as hostile. After the U.S. and Israeli attacks on Iran, Iraq's prime minister **declared** the war "unjust" and refused to allow the country's territory to be used as a base for U.S. strikes. Iraq also **blocked** Iranian Kurdish rebels from using Iraqi territory for attacks on Iran, which the Trump administration and Israel had endorsed at times. Because the Iraqi government often works closely with Iran, Tehran does not see Iraq as an enemy as it does Saudi Arabia and the UAE.

Iraq and Iran-backed militias may consider Kurdish-operated fields, foreign companies, or sites perceived as associated with the United States as more acceptable targets than infrastructure controlled only outside the Iraqi Kurdish region. During the war, Iran has expanded **attacks** to energy infrastructure in the Kurdistan region. Iran also **attacked** Iranian Kurdish rebels based in Iraq after the start of the war in February, with attacks continuing through July.

In general, countries suffering from considerable civil strife are far more vulnerable to attacks on oil pipelines and other infrastructure. Part of this is simply the presence of large numbers of armed groups that seek to disrupt oil income flowing to their enemies or use the threat of attacks as a way to blackmail oil companies into handsome payouts. In addition, governments suffering civil wars tend to be weak, and their lack of control over much of their territory offers many opportunities to strike at isolated pipelines and other infrastructure. For example, jihadist terrorism and Shiite-Sunni violence in Iraq after 2003 involved hundreds of attacks on energy infrastructure so **devastating** that they have hindered the development of the industry to this day.

Iran-backed Shia Muslim groups in Iraq **struck** U.S. targets in the current war, ignoring Iraqi government efforts to stay neutral. The militias also launched drones at oil infrastructure sites in Saudi Arabia, such as oil fields and a refinery in the Yanbu oil hub, leading Saudi Arabia to strike these militias in Iraq. Regional sources **claim** that up to half of the UAV attacks during the war have come from groups in Iraq. Houthi groups based in Yemen also **attacked** Saudi Arabia from there.

Saudi Arabia, the UAE, and other Gulf States

Tehran considers both Saudi Arabia and the UAE to be enemies and is also hostile to other Gulf states. The UAE, in particular, has supported strikes on Iran, reportedly conducting dozens of airstrikes on its own (including on **oil infrastructure** in Iran) and **hosted** U.S. forces. Saudi Arabia has also been an important, if quieter, supporter of these attacks. At the same time, Iran has far less capacity to conduct attacks from within Saudi Arabia, the UAE, and other Gulf states than it does in Iraq, and these countries have better air defenses.

However, the Gulf countries are not a unified front. The Gulf Cooperation Council itself issues joint statements, but in practice the member countries often go their own ways. In response to economic pressure stemming from potential Iranian attacks on its LNG industries, Qatar **tried** to offer Iran covert support in exchange for guarantees that it would not attack critical infrastructure. The UAE has both attacked Iran and, despite bearing the brunt of Iranian counterattacks, **Reuters reported** in June 2026 that the UAE had agreed to make billions of dollars available to Iran as part of a de-escalation arrangement that coincided with U.S.-Iran ceasefire negotiations, although Abu Dhabi categorically denied that it had transferred or released any funds.

Iran has regularly demonstrated its willingness to attack energy infrastructure in the Gulf states, both to disrupt energy supplies and put pressure on the U.S. government. Tehran has also regularly targeted U.S. military facilities in the Gulf. Iran has **attacked** the UAE more than any other country in the latest war, making

the UAE-Israel partnership even stronger. In addition, Gulf states' air defenses have shown themselves to be able to cover part of a country, but not all of it—and extensive oil infrastructure offers many targets.

Saudi Arabia has **championed** negotiations more vocally than the UAE and has otherwise been less willing to be openly associated with Israel, despite still supporting the U.S. and Israeli military campaign. Indeed, Saudi Arabia has also **conducted** several retaliatory attacks on Iran and Iranian-backed groups in Iraq with its own forces, though it has sought to keep them low-profile. Bahrain and Kuwait have, in general, **followed** the Saudi diplomatic line and sought to keep their own roles limited.

At the same time, none of the Gulf monarchies are dealing with an active insurgency, pro-Iran groups linked to their governments (such as the Popular Mobilization Forces in Iraq), or other factors that give Iran so much influence in Iraq. Gulf state intelligence services have long prioritized countering Iranian-backed subversion, and while Tehran may maintain some networks (Bahrain **regularly claims** that it disrupts Iranian agents), these are probably not extensive.

Implications for the United States and Its Allies

Gulf oil exporters often must conduct costly and lengthy repairs when oil and gas infrastructure is damaged. As repairs are underway, companies must choose between rerouting oil and gas from damaged infrastructure, reducing production, or holding resources in storage. Over the long term, the costs associated with attacks and repairs may heighten internal security concerns and provide Iran leverage over Gulf countries and Western companies.

Physical Damage and Repairs

The scale of immediate physical damage caused by an attack on oil and gas infrastructure depends on planning, capability, and luck. Two similar UAV strikes targeting the same infrastructure can have radically different outcomes—from a minor rupture to a major explosion—based on where the UAV happens to hit. However, actors with better technology, targeting intelligence, experience, and knowledge of vulnerabilities are more likely to cause severe disruption. Multi-target attacks, in particular, have compounding impacts that are more difficult to manage.

Recovery and repair capabilities determine much of an attack's impact. Recovery can be strengthened by well-equipped repair teams or hindered by crews that are lacking experience or overburdened. Specific damages require specific repair skills, making matters complicated: A repair team knowledgeable in

fixing a damaged pipeline may be unable to cap a wellhead. Proper materials for repair must be available in advance, or easily accessible, to avoid procurement delays. Lastly, attacks or the risk of attacks on repair crews themselves can bring work to a halt. All of these factors make repair estimates difficult, but past repair performance serves as the best available—albeit imperfect—guide for the prediction of future threats.

Attacks targeting onshore wellheads often cause lasting damage and involve specialized repair teams. Resulting fires **can burn the reserve** that the wellhead is tapping, requiring capping expertise that can take weeks to deploy. Mass attacks are especially damaging, as demonstrated by the Kuwaiti oil well burnings during the first Gulf War, when over 700 exploded wellheads **burned** over 1 billion barrels of oil and took international experts around nine months to cap. In addition, attacks on gas-oil separation plants **can take months** to repair. Offshore infrastructure takes even longer to repair because of transport logistics issues, including the supply of replacement parts.

Upstream and midstream processing facilities host massive and specialized equipment that can require long replacement and repair times when damaged. Exact repair details for strikes on these facilities are often not publicly available **for security reasons**. Nevertheless, gas plants or LNG terminals generally require longer repair times than oil facilities. Iranian-linked attacks in **2019** and **2026** on the Abqaiq processing mega-plant, which largely handles oil, only led to limited damage, while missile attacks on the Ras Laffan LNG terminal in Qatar in mid-2026 disabled high-capacity trains that will **reportedly** take until 2027 to fix.

Crews normally address individual explosive attacks on pipelines within hours or days, whereas attacks on pumping stations take longer because the stations have more complicated equipment that must be replaced and recertified. Attacks on pumping stations in the region have been devastating in the past: For example, the U.S. bombing of a Kirkuk-Ceyhan pumping station severely **reduced** the line's capacity during the coalition invasion. During the Six-Day War between Israel and its neighbors, an unattributed **bombing** on a pumping station for a pipeline linking Iraqi oil to ports on the Mediterranean and Red Sea led to the line being taken offline permanently.

On the other hand, attacks along multiple points can put the pipeline out of commission for long periods. From 2003 to 2008, for example, Sunni insurgents in Iraq **staged** hundreds of attacks on internal pipeline systems, debilitating the regime's capacity to earn income and stunting the postwar rebound of the country's oil industry. ISIS militants employed a similar tactic following their 2014 takeover of much of the northern part of the country, destroying many critical pipeline systems. Similarly, companies facing already decaying pipelines may take weeks or months to reestablish flow.

Two similar UAV strikes targeting the same infrastructure can have radically different outcomes—from a minor rupture to a major explosion—based on where the UAV happens to hit.

Export terminals and loading zones are the other main pieces of infrastructure, besides pipelines, that are involved in transit; they usually do not present extensive repair delays following isolated UAV attacks. Attacks on **Saudi**, **Iraqi**, and **Emirati** terminals, for example, all have caused limited damage repairable within a few days. However, heavier attacks on terminals—or on refineries located near them—may require longer repair times. Lastly, offshore loading terminals remain vulnerable; these artificial islands can require **months-long repairs** if they sustain damage from bombings, missile strikes, or UAV assaults, and they are critical chokepoints for the loading of oil onto tankers.

Effects of Network Disruption

Some attacks pose extreme threats to entire oil and gas networks. Infrastructure that handles significant flows of oil and gas without easily available alternatives is vulnerable. This category of critical vulnerability includes export terminals, large upstream and midstream processing centers, and large overland or undersea pipelines. Downstream refineries are important for getting oil and gas to consumers and are especially critical points.

However, large infrastructure with easily implementable alternatives—even if they are more costly—is not as vulnerable. Buildup of excess processing capacity and alternative pipeline and export routes, as has been implemented in Saudi Arabia, can mitigate much of the harm caused by an attack by preventing network stress at times when peak capacity is diminished.

Infrastructure that handles less significant flows is not as critical to networks and usually has implementable alternatives. Nevertheless, campaigns of attrition—such as covert sabotage on the ground, spanning years—can significantly weaken industry. Infrastructure that is directly related to extraction—wellheads, separation tanks, and initial pipelines—can be degraded in ways that lead to long-term losses or stalls in network capacity.

Internal Security Fears

The 2026 attacks by the Houthis and Iranian-backed Shia militias in Iraq demonstrate that Tehran-backed groups can threaten Gulf country oil infrastructure. In the postwar period, Iran is likely to double down on these groups and may seek to create cells within the Gulf states themselves that could, among other tasks, attack oil and gas infrastructure.

The very threat of such clandestine operations is likely to increase internal security concerns in the Gulf states. This may involve greater intelligence and law enforcement efforts against suspected Iranian cells and agents of influence, but it might also lead to greater crackdowns on dissent in general.

Increased Iranian Leverage

Iran has demonstrated its ability to cripple the oil and gas output of some regional actors, and this will increase its potential coercive leverage in the future. Iranian successes may cause countries to reconsider their diplomatic positions, including cooperation with the United States (especially overt military cooperation), relations with Israel, and the provision of financial relief to Iran.

After the war, some Gulf countries wishing to protect their bottom lines and shore up security may toe a line that is more pro-Tehran to prevent conflict. Others may simply attempt to establish new rules of engagement with the Iranian regime, including red lines on oil and gas infrastructure in exchange for diplomatic, economic, and security concessions. Still others may look to the United States for additional security assistance.

Cautious Western Investment

Iran's proven ability to attack Western company assets may drive up the cost of business for Western companies, putting them at a potential disadvantage relative to non-Western corporations and discouraging investment in the region. U.S. companies themselves may begin to look at investments in the Middle East with more concern than in the past. Chevron, Exxon, Shell, and other Western corporations hold partial stakes in many Middle Eastern oil projects. Iranian attacks on Western-owned or associated facilities have been common throughout the war and are a persistent threat moving forward.

In response, Gulf countries and Iraq may begin to think twice before encouraging U.S. involvement in oil and gas projects or infrastructure projects generally, viewing them as more likely to attract Iran-linked attacks. This is particularly likely if Gulf governments and Iraq can find alternative commercial and security partners.

Conclusions

The United States and its Gulf partners should prioritize a layered approach to protecting energy infrastructure against Iranian threats. Because traditional air defense interceptors are expensive and finite, the United States should accelerate development and deployment of lower-cost, low-altitude defenses while also replenishing critical interceptor stocks. Interception, however, will

never be perfect, and the dispersed nature of oil and gas infrastructure means that protecting one site may simply shift attacks elsewhere. In addition, if the cost ratios continue to favor the aggressor, then the Gulf states and the United States may spend heavily to achieve only limited results. Governments and companies should therefore improve surveillance and physical security at particularly vulnerable and difficult-to-repair upstream nodes, including high-flow wellheads, gathering and separation facilities, oil rigs, pipelines, and other chokepoints.

Resilience and rapid recovery should complement these defensive measures. Gulf producers should expand inventories of critical spare parts, develop specialized rapid-repair capabilities for damaged pipelines and processing facilities, and maintain sufficient spare production and transportation capacity to compensate quickly for disruptions elsewhere in the network. Future pipelines and energy facilities should be designed with security in mind, with attention paid to the vulnerabilities created by remote desert locations and identifiable single points of failure. ■

***Daniel Byman** is the director of the Warfare, Irregular Threats, and Terrorism Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C. **Alden Ness** is a former research intern with the Warfare, Irregular Threats, and Terrorism Program at CSIS.*

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

The authors would like to thank Hunter Macdonald for her careful editing, Aidan Skidds for his research assistance, and Karen Young for her comments on a previous version of this report.

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

© 2026 by the Center for Strategic and International Studies. All rights reserved.