Ferndon Consulting LLC
team@ferndon.com
https://ferndon.com

Initial projections for economic and societal sectors following Operation Epic Fury on 28 February 2026

Publication Date: 02 March 2026

The U.S. and Israeli military attack on Iran (Operation Epic Fury, 28 February 2026) is likely to have compounding and evolving effects. Preliminary analysis drawn from a wide variety of sources highlights some key considerations in the weeks ahead. This is general and by no means comprehensive. More nuanced and focused insight is available.

Facts and Assumptions: Click Here

Sectors:

- Critical Infrastructure: Click Here
- Criminality: Click Here
- Defense Contracting: Click Here
- Emergency Management: Click Here
- Financial Institutions: Click Here
- Humanitarian Organizations: Click Here
- Manufacturing: Click Here
- Policy Makers: Click Here
- Security: Click Here

FAQ: Click Here

Facts and Assumptions:

These factors shaped the context from which our information was analyzed to identify significant geopolitical nodes that shape vulnerabilities and priorities. The vulnerability is where we are most likely impacted; the priority is that which we need to preserve. The greatest impacts by an attacker come through affecting the most vulnerable point with the greatest impact. Key considerations are tied to:

1. Strait of Hormuz is a significant logistical choke-point: traveling through this region during conflict is a high increase in risk both due to the likely proliferation of unexpected weaponry and due to probable direct impact to opponents' supply chains and resources. The Strait of Hormuz is currently closed, but the duration and impact of this shutdown is still a developing situation.
2. The IRGC and their Quds force are the dominant power in Iran. The IRGC has clearly stated that it will activate its cells in response to any attack on Iran, as well as attack U.S. and Israeli sites in the Middle East. This assumes both that sleeper cells / recruits are located within the U.S. and that sleeper cells / recruits exist in communities that are often not aware of their existence.
3. U.S. Congress is debating DHS funding. ICE restrictions are also under review.
4. Conflict in general has evolved from traditional force on force clashes. Most recent conflicts are simultaneously engaged both through conventional military and through attacks intended to undermine population, supply chain, and communication infrastructure resilience. It is extremely likely that response to the attack on Iran will not be restricted to military engagements.
5. Cyber-attacks across critical infrastructure and society are highly likely to increase during time of international strain and conflict. Some predictable effects of cyber-attacks include resource diversion and draining, supply chain impacts, long-term damage from data breaches and operational damage. Phishing and ransomware attacks often increase in the aftermath of disasters or wherever resources are being strained or re-allocated. However, insider threats are also a rising concern.
6. There has been a world-wide increase in extreme weather events. If the Southern Hemisphere summer is a marginally accurate predictor of our 2026 Northern Hemisphere summer, we expect a very hot summer with much of the USA already in drought conditions. Research published through Applied Energy emphasized that cyber-attacks or sabotage of critical infrastructure during or after a significant weather event compounds potential impact of the attack by at least 3x.
7. Russia and China, both economic allies of Iran and members of BRICS, are not overtly coming to Iran's defense or interfering. However, this does not mean that they or their agents will not use the situation to their advantage in undermining competition.
8. Iran is actively targeting Middle East infrastructure primarily, inclusive of civilian and economic.

Sectors:

Criminality: Criminality is likely to take advantage of this time of decreased accountability and increase activity. The increasingly raised social tensions decrease witnesses' likeliness to volunteer as witnesses to crime, especially in light of the deportation concerns. This can range from petty local crime to cyber-crime to transnational criminal crime. For potential victims of crime, trust in local security, emergency response, and law enforcement will be key. While the big picture is shifting and big threats loom on the horizon, smaller petty crime expects lower accountability and surveillance.

Critical Infrastructure: Targeting of Critical Infrastructure is increasingly likely. Critical Infrastructure is a widely advertised ideal target for terrorist cells, is vulnerable, is in constant demand, and impacts a high number of civilians – in addition to providing support to military operations. Additionally, Iranian hacker elements have already officially stated that they will be targeting U.S. critical infrastructure in retaliation for this attack on Iran. According to NSA, "Since October 2023, Iranian cyber-actors have used a technique known as brute force to compromise (critical infrastructure) user accounts and obtain access to organizations to modify MFA registrations, enabling persistent access." The energy grid is vulnerable to both cyber-attacks and direct sabotage: sabotage can be as easy as falling a tree on transfer stations or running a truck into a key supply point. Water lines are increasingly lucrative targets, especially when response is impacted by snow build-up and freezing weather; not only the cyber-security needs to be maintained, but also physical security and increased testing for contaminants may be advisable given poisoning water sources is another recommended terrorist act. A broken main line can contaminate an entire community's drinking water. Communication is already being exploited and is vulnerable, especially the cellphone networks and large internet servers; communication infrastructure is a prioritized target. Railroads have been intentionally targeted in the Russian-Ukraine conflicts by sabotaging track; runaway trains have been advertised as an excellent tool for a large, deadly missile on a set trajectory. Healthcare is struggling to maintain manning following the COVID-19 pandemic and does not have significant professional redundancy. On top of that, the HHS Office of Civil Rights stated (in April 2025) that ransomware attacks on healthcare have surged by 264% in the last 5 years. CSIS emphasized that maritime ports are a cornerstone of the international economy. Impacting the port through cyber or physical sabotage can affect perishables, medical supplies, and military responsiveness: successful attacks on a port can have among the widest impacts on human populations.

Defense Contracting: Defense contracting is likely to endure both highs and lows. The Iran conflict will likely be profitable for the larger contractors with broader flexibility and ability to shift with government need. Smaller subcontractors are more likely impacted, and effects will travel along the supply chain, impacting not only the subcontractor but also those they supply with parts further along the supply chain. Missiles or other indirect fire production orders are likely to continue or increase. Simultaneously, there is likely to be increased Counterintelligence threats. Compliance with security (such as the CMMC compliance) will be of increasing

importance. Collection, sabotage, and blackmail are all means to gain control or influence of defense supply sources at any accessible and vulnerable point on the supply chain, inclusive of suppliers outside the United States. Insider threats continue as a legitimate vulnerability.

Emergency Management: Planned human-made emergencies are likely to seek maximization through either compounded emergencies or taking advantage of social unrest: this increases the potency and drains the emergency response teams. Lone Wolf shooters and irregular bomb threats are not unexpected: while there is the chance for a Black Swan event being triggered from this incident, that is less likely than many smaller, dispersed, and erratic events in the U.S. at this point. In general, the most devastating event would be tied to chemical/biological materiel contaminating the water, air, or food than a nuclear event. If there is any uptick in the U.S. of actual or probable terrorist cell activations, it is strongly recommended to ensure Emergency Management is autonomous from Security or Emergency Response. While minor incidents may be addressable by a chief of security acting as the emergency manager, compounded threats, such as a cyber-attack on the critical infrastructure during a weather event, necessitate security to function as security and an independent Emergency Manager coordinating resources and assets that go beyond typical Emergency Response.

Financial Institutions: Financial crime is likely to increase. Immediate impacts from increased cyber-attacks targeting U.S. & foreign banks could include, but would not be exclusive to, interruptions in banking services that impact global payment networks for consumer and corporate transactions outside Iran since US banks cannot transact with any Iranian entity economic impacts and payment problems, and ATM disruptions. Iranian and Iranian-affiliated businesses are highly likely to shift their funds, assets, and liabilities.

Humanitarian and Religious Organizations: This is a time for opportunity and a time for educated awareness. There is likely to be increased scrutiny of populations with history or reporting that associates them with terrorism. Refugees, immigrants, and certain communities could be, unbeknownst to them, harboring unidentified terrorists or radicalized community members. However, community organizations could also be exploited: there have been instances of antagonists and terrorists using a religious site as a place of refuge and a place from which attacks can be launched.

Manufacturing (general): The greatest impact to manufacturing, outside security considerations, is likely to be slightly delayed and impact on the supply chain that includes need for petroleum products, inclusive of lubricants (directly and indirectly) and plastics. Two primary factors that affect manufacturers' bottom line are: (1) affected traffic through the Strait of Hormuz and (2) decreasing trust in U.S. entities as trading partner. Lubricants and plastics are often forgotten heroes in the manufacturing supply chain: most points in a supply chain wherein components are manufactured uses both plastics and lubricants. If the conflict with Iran resolves quickly, this shortage may be absorbed by various points in the supply chain with redundancy from alternative sources or reserves – if the conflict is extended, the prices for petroleum

products is likely to rise as the supply chain shifts route. As discussed in more detail in our recent Manufactures publication, discussion and re-alignment of customers and sourcing within the manufacturing supply chain is increasingly likely now due to perceptions of U.S. market volatility. These perceptions of volatility come from tariffs, changing policies, and increased military actions. Attacking Iran ties directly to the concern regarding military actions and is likely to tie indirectly to future policy changes and tariffs.

Security (cyber and physical): IRGC-sponsored terrorist cells are likely to be activated in retaliation to the attack on Iran. This is inclusive of both physical and cyber-security threats. These cells are widely dispersed and have sleepers capable of physical access and sabotage, embedded in a wide range of research labs, critical infrastructure, academic institutions, religious organizations, prison systems, law enforcement organizations, and other entities. Physical access may enable a range of impacts from (1) simple information operations to (2) direct physical uploading of viruses (bypassing many cyber-security measures) and even (3) physical action on a target, such as sabotaging a dam or undermining safety measures in a nuclear reactor. Regarding the cyber-security threat, Iran and her proxies have a robust cyber-capability that is operational. Likely attack vectors, well organized by Sentinel One, are being actively disseminated, but do include DDoS attacks, website defacement, PII theft, wiper malware, and even destructive viruses (similar to Stuxnet). In the interim, CISA has been reduced. But even in January 2026, not only was CISA advertising a need to increase cyber-security, but it was also highlighting the need to increase insider threat programs through multi-disciplinary threat management teams.

Policy Makers: The attack on Iran is likely to impact DHS funding, ICE operational parameters, and tariffs. If there is a credible threat to the homeland – and IRGC threat to activate cells does constitute a credible threat to the homeland – DHS funding is likely to be released and increased. Further, as many cells' manning can include immigrants, refugees, and citizens, operations to mitigate likely threats will be justifiable. Jurisdiction for known migrant-occupied "no-go zones" such as communities within the Islamberg network, has been with DHS: these sites are a reasonable launching point or support node for terrorist cells.

Frequently Asked Questions (FAQ):

Will the attack on Iran affect my bottom line?

The attack on Iran is highly likely to affect your bottom line if your supply chain is directly or indirectly impacted. Direct effects would be your shipments traveling through the Strait of Hormuz being waylaid, delayed, or lost. Indirect effects could be your supplier running out of lubricants, your supplier shifting customers due to decreased faith in the American Market or changed policies that affect your supplies or market. Additionally, bottom lines are likely to be impacted by short-term liquidity challenges that are likely to materialize, both in terms of access

to and cost of short-term cash requirements. Dampened economic growth will also impact a company's forecasts and performance.

How can I determine if my ROI will be impacted by the attack on Iran?

There are several ways you can determine if your ROI will be impacted by the attack on Iran. First is knowing your supply chain. You can analyze your suppliers, their routes, and their personnel. This is for both your direct suppliers and for those who supply them with materials to make the component they provide your organization. Do not forget to add cultural nuances into this consideration of supplier: if you supplier is a member of a "face saving culture" or one who has been struggling with U.S. policies, it is likely they may be considering alternative markets. Second, you can look at your market to determine the stability of your product. Is your market sold in the U.S. or overseas? If overseas, what are the general atmospherics of that country to U.S. produced goods? Third, know the security of your host servers and be aware of those who are hosted by others along your supply chain. The high likelihood of a cyber-incident after a military strike re-enforces the need-to-know which server and where, the security, and even the locality of those servers. Fourth, you could make this easier and call the team at Ferndon (literally: team@ferndon.com) who can help break this down with the very detailed nuances at each point with a third party perspective (and an NDA).

Will the Strait of Hormuz be shut down due to the conflict in Iran?

It already is. When it re-opens for the initial trade, the Strait of Hormuz is likely to experience slowed down and/or more expensive traffic due to threats of violence. The risk for ships going through a conflict zone increases with threats of terrorist cell activations around the ports, missiles being fired in the area, and piracy. Given the increased risk, shipments may be consolidated, delayed until the conflict cools, be required to pay outrageous insurance fees, or have additional security hired. Materials traveling through the Strait of Hormuz – such as petroleum products – have both redundancies and surpluses along the supply chain. However, if the conflict drags on, these products (plastics, lubricants, petroleum) will likely decrease in availability.

How badly do we expect the U.S. to be hit by attacks?

We do not expect the U.S. to be crippled by retaliatory attacks. There may be critical infrastructure attacks, but widespread outages and disruptions are very unlikely in the U.S. at this time. We have a complex regulatory environment for electrical generation and distribution as well as disparity between grids and power distribution hubs. It is likely that even if there are blackouts in any given area over the next few weeks, few if any people will actually know the root cause. So yes, while there will be IRGC/Quds-sponsored cyber-attacks, they will likely come from 19–25-year-olds with limited resources and access hitting targets of opportunity. This does not mean they will not hit a bank or two or take an ATM offline, etc. But widespread outages are unlikely. Will they disrupt GPS systems and comms systems in the Middle East?

Absolutely (they already are). But will they take the U.S. internet offline? Highly unlikely. The U.S. doesn't have single points of national failure. The biggest threat from cyber or kinetic attacks will be in the Middle East – any U.S. interests there, inclusive of supply chain sourcing, are at highest levels of risk.

Will the U.S. simply invade Iran?

Very unlikely. The return on investment would be atrocious for the USA: Iran is a strong, proud, educated, technologically advanced country. Any invasion of Iran would galvanize the population against us. And it would not be pretty.

How long will this conflict with Iran last?

The duration of this conflict is in the air right now. There is an initial power vacuum if the reports of the Ayatollah's demise are accurate. The conflict could be resolved soon or be dragged out. If concerned about "return to normal operations" and a stable supply chain and market, the question is not necessarily how long *this* conflict will last. Another and maybe better question would be: how significant will the after-effects impact my ROI? Given the increasing concern about reliability of the U.S. as a trading partner and wide-spread concern of the internal stability of the U.S., it is very likely that multiple nodes within the supply chain are intentionally diversifying their market to reduce dependence on U.S. markets. This could have significant and long-lasting effects.

Will you be publishing future U.S. military action predictions?

Absolutely not. We might be speaking with our customers about what is likely coming; however, Ferndon Consulting values our brothers and sisters in uniform. We will not ever make a statement or share information that could create a negative impact on our military. To those old-school readers who understand this: we have our Purple Dragon OPSEC signs in the office.

What's the absolute worst "reasonably possible" scenario for which we should prepare?

An attack on the energy sector that powers essentials in a high-density urban environment with a current low trust in government during a significant weather event. So, ConEd and friends, thank you for keeping up the good work!

Can I use AI to project my future planning instead of paying a person?

AI can help with your planning, especially in predictable environments. When time is of the essence, very few AI programs can integrate nuanced and rapidly changing dynamics for rapid responses. AI methodically learns and is strongest on more static questions with established data points. Future projections are feasible but often insufficiently nuanced with international perspectives to plot likely or feasible behaviors trans-cultural and trans-societal behavior. Additionally, material needs to be added to the internet for the AI to read, and that materially should be formatted in a manner where the AI is able to read, analyze, and then integrate: much

of our writing is not formatted for AI search engine optimization or is re-written for this optimization by another AI. It is strongly advised to work closely with cross-functional SMEs, well-versed in geopolitics and understanding of how to read what is happening and, within this dynamic context, the likely future evolutions.

How can a geopolitical expert, such Ferndon Consulting, help?

Cross-functional fusion intelligence is exceptionally helpful in navigating dynamic geopolitical change. As the internet waits for information, processes that information, and then provides you input, the SMEs at Ferndon can give you direct and timely analysis that is more nuanced and refined than that which would be consolidated by AI. If you're looking for an "azimuth check" or contextual development, we are happy to talk, receive your concerns, provide context, and support your need. We do recommend aligning a fractional arrangement or subscription to products: we value trust and want you to have the best information available with a positive relationship with the provider.

How would an initial consultation with Ferndon Consulting go?

First, talk to us and determine whether we should collaborate: that's free. We care about your trust, and we are happy to sign an NDA at any point in the proceedings. When you come to the initial consultation, we ask that you bring your situation, your needs, your end-state, your concerns, and your restrictions. We can identify initial considerations and likelihood that we can help you – and bracket the probable extent to which we can assist. If you wish to proceed, we would then come up with a plan: if immediate support (such as mitigating risk during this current evolving situation in the Middle East), we are happy to align a contract that includes that immediate support and, as we work together, build future plans and follow-on contracts. If you're looking for more fractional geopolitical support, building towards the future, we would be happy to propose a pilot or subscription option.

Where can I sign up for future updates?

Our newsletter and many of our general updates are free: go to our website (https://ferndon.com) and, at the bottom of the page, there is a sign-up for our newsletter spot. We often also follow up with a post on LinkedIn. Easy peasy. Or you can set up fractional, subscription, or other support that is specific to your situation: if a significant situation emerges, we reach out directly to you and are available, personally, to help navigate future situations.