THE CHERTOFF GROUP

POINT OF VIEW

The Death of Qassim Suleimani and Risks to Global Security

What happened?

On January 3, 2020, a U.S. drone strike near Baghdad airport killed Maj. Gen. Qassim Suleimani, one of Iran's most powerful military commanders overseeing security and intelligence, and close confidant of Supreme Leader Ayatollah Ali Khamenei. Suleimani ran the Islamic Revolutionary Guard Corps Quds Force – the branch dealing with foreign operations – and was the architect of much of Iran's asymmetric warfare techniques and influence peddling via Shiite militias throughout the Middle East in recent years. In April 2019, the Trump Administration formally designated the Quds Force as a foreign terrorist organization.

Why it's important

Given his stature within Iran, Suleimani's death brings one of the most significant escalations in U.S.-Iran relations in the last forty years. Ayatollah Ali Khamenei has called for "forceful revenge" for the killing. Domestic pressures within the Iranian regime and the perception of fraying Iranian influence and control in Iraq and Lebanon are likely to feed the motivation of the Iranian leaders to retaliate. There is now heightened potential for a broader conflict which could flare up in multiple corners of the globe unpredictably, inviting miscalculation.

What's next?

Under the circumstances, The Chertoff Group believes retaliation is a question of when, not if. While Iranian intelligence traditionally takes its time planning operations, there will be mounting pressure for an in-kind response in areas where Iran can easily extend its reach. Such an event could have major implications for U.S. private sector organizations and civilians – primarily but not limited to Iraq, Syria, Lebanon, and Afghanistan. Other Middle East and South Asia nations where Iran has operated before and where they have influence either directly or via proxies should be considered, including Gulf States, Pakistan, Turkey, Argentina, Thailand, or Austria. Israel, for its part, faces hostility from Iran on par with the U.S. and is likely to be targeted.

Therefore, it is prudent to assess the risk landscape and evaluate likely avenues Iran may take to attack and inflict harm on American citizens in the Middle East and elsewhere. The following represents several scenarios likely to play out in the short to medium term, leveraging both physical and cyber attack vectors, based off Iranian capability and intent.

Physical Attack on U.S. Targets

Before his death, reports highlighted that Suleimani had ordered the movement of ground-to-ground and shoulder-fired surface-to-air missiles to Iraq to be used by proxies against U.S. military targets. In the aftermath of Suleimani's death, a military or diplomatic target is one of the most likely scenarios that Iran would clearly see as commensurate with its loss. Anything less will look weak at a time when the regime in Tehran is already facing domestic pressure. To the extent that American facilities are strongly fortified in Iraq and the wider Middle East, Iran may try to attack where an American presence is less protected. If preferred targets such as military installations are deemed too difficult to strike, Iran or Iranian proxies are likely to devolve to softer targets, such as companies symbolic of the U.S., civilians, and foreign employees of U.S. companies.

Moreover, an attack by Iranian proxies in the United States is not out of the question. Iranian-backed attackers have previously targeted officials in the United States, most notably during a failed 2011 plan to assassinate the Saudi Ambassador to the United States at a restaurant in the Georgetown area of Washington, D.C.

Drones and Ballistic Missiles

The September 2019 attack on Saudi Arabia's Aramco facility highlights the role unmanned aerial systems (UAS) can play in carrying out debilitating attacks on critical infrastructure facilities. The incident featured a combination of alleged Iranian cruise missiles and UAS, which Saudi air defense systems were unable to defeat. Over the course of just 17 minutes, the attack demonstrated just how vulnerable a critical piece of national infrastructure can be from this type of air attack. Drone strikes will continue to be a viable option for an Iranian response.

Additionally, given Iran's sizeable ballistic missile arsenal, rocket attacks and the potential threat of short-range ballistic missiles present an ongoing challenge for Israel, the Gulf States, the security of airspace and shipping lanes, as well as American installations within target range. Aside from security implications, this situation may prompt new investments in air and missile defense (IAMD) systems.

Hostage Taking

Iran has a history and preference for taking hostages and holding them as bargaining chips. The Quds Force is experienced in this tactic, particularly in the Levant where proxies are strongest and have the most freedom of movement. Hezbollah, based in Lebanon but with the ability to conduct attacks abroad, remains a particular threat. The U.S. government has already ordered

civilian evacuations in Iraq. While the situation remains dynamic, U.S. citizens in the Middle East should exercise vigilance and be on high alert.

Sleeper Cells and Insider Threats

Iran operates sleeper cells throughout the world precisely for the purpose of attacking targets both in the Gulf Region and beyond during a time of escalation. These representatives conduct pre-attack surveillance operations, recruit, and funnel money to pro-Iranian groups. Suleimani spent years managing and consolidating the various pro-Iranian proxies dispersed worldwide. U.S. corporations, particularly those with facilities and personnel in the Middle East, should review insider threat procedures, as this poses a particularly attractive attack vector, especially in high risk industries like aviation. Lone wolf attacks inspired or directed by Iran could play an increasingly prominent role if the crisis escalates.

Strait of Hormuz

Given Iranian naval power and the proximity of the Persian Gulf, increasingly bellicose action in the Strait of Hormuz remains a distinct possibility. Throughout 2019 Iran demonstrated its capabilities to disrupt shipping activity across one of the world's most important oil gateways, causing temporary spikes in oil prices. It has also frequently cited its willingness to close the Strait. Some level of disruption to shipping is likely in the near term as part of Iran's response, with implications for U.S. allies like Saudi Arabia and the UAE, as well as companies doing business there. While a direct attack on foreign shipping either from Iranian vessels or missile sites is less likely, mines present a more challenging scenario.

Cyberattack

The Chertoff Group believes that a cyber attack targeting U.S. federal, state, local governments, critical infrastructure and foreign allies is a likely course of action. To some extent, these are reportedly already occurring, though cyber attacks alone are unlikely to be judged sufficient by the Iranians to constitute revenge for Suleimani's death. Iran has a history of targeting both public and private sector information technology (IT) and operational technology (OT) (e.g., industrial control system) networks for intelligence collection and disruption, as well as generating kinetic effects through cyberspace. Iran has also historically targeted the U.S. financial sector.

In particular, U.S. state and local government entities, critical infrastructure asset owners, and operators in the United States, Iraq, Saudi Arabia, and other U.S. allies in the Gulf region should be wary of increased intrusion attempts, network availability attacks, and data interception or destruction operations against both enterprise IT and OT networks within their organizations

and business partners. Of note, the attacks described below are reasonably foreseeable retaliatory courses of action given previous activity linked with Iran.

Wiperware: In one of the earliest attacks attributed to Iran, destructive malware attacked the computer systems of Saudi Aramco in 2012 (on the eve of an Islamic religious holiday). Once a machine is compromised, the Shamoon malware works to spread to other devices across the network, and in Aramco's case overwrote data on 30,000 computers.

Ransomware: In 2018, two Iranian individuals were indicted for conducting computer hacking and attempted extortion over a 34-month period. The pair allegedly developed and deployed a sophisticated ransomware encryption campaign – "SamSam Ransomware" – against more than 200 state and local governments, public institutions and hospitals. The Iranians attempted to extort payment through demands of cryptocurrency from affected agencies in cities such as Atlanta, GA, Newark, NJ, and San Diego, CA; educational institutions such as the University of Calgary in Alberta, Canada; and hospitals and healthcare entities such as LabCorp, MedStar Health, and Allscripts Healthcare Solutions among others. While the indictment of these individuals does not link them to the Iranian government and/or the IRGC, it would indicate that the know-how to conduct such a sophisticated and debilitating attack exists within Iran. Such know-how could be deployed for a wide range of objectives targeting state, local and private sector organizations, including but not limited to the upcoming 2020 Presidential election season.

The success of recent ransomware targeting, Iran's experience with Shamoon – combined with observations from the far-reaching economic impact of Russia's 2017 notPetya attack in Ukraine – all suggest some form of disruptive/destructive malware attack as reasonably foreseeable.

DDoS: In 2016, seven Iranian individuals, employed by companies affiliated with the Iranian government and the IRGC, were indicted for conducting a prolonged, 176-day DDoS campaign against 46 victims mostly within the U.S. financial services sector. The campaign, waged between 2011 and 2013, crippled some customer-facing banking websites, preventing access to banking services and customer accounts and costing the institutions "tens of millions of dollars in remediation costs."

Supply Chain: In late 2018, it was discovered that hackers (linked by security researchers to Iran) intercepted sensitive data over a two-year period from telecommunications service providers, Internet service providers, government organizations, and other institutions across the Middle East, North Africa, Europe, and

North America through the manipulation of domain name system (DNS) mechanisms at scale.

Operational Technology: Late in 2019 to the present, our strategic partner Dragos, a leading industrial cybersecurity and threat intelligence provider, reported on disruptive cyber activity targeting OT asset owners and operators in the oil and gas industry there were likely linked to Iranian targets. Iranian cyber attack group APT33 (or "Holmium," "Refined Kitten," "Elfin") could be shifting focus from IT-focused attacks to OT-focused physically disruptive attacks through use of wide-ranging and complex "botnets" that conduct "password spraying" against manufacturers, suppliers and companies that maintain industrial control systems.

This follows reports that in 2017, an attacker successfully deployed malware that, were it not for a programming error, would have disrupted industrial safety systems at a large Middle Eastern petrochemical facility, triggering an explosion.

For questions or clarifications needed on this or other global security risks to commercial entities, please contact:

Brogan Ingstad, Associate

brogan.ingstad@chertoffgroup.com

202.552.5267