AMERICAN FOREIGN
POLICY COUNCIL

Iran Could Still Strike Back at the U.S.

January 20, 2020 *National Review*

Related Categories: Democracy and Governance; Economic Sanctions; Human Rights and Humanitarian Issues; Islamic Extremism; Iran

How might Iran respond to the death of Qasem Soleimani? Ever since the Trump administration's January 3 killing of Soleimani, the Islamic Republic's top military commander, that question has been on the mind of policymakers in Washington and the American public at large.

Iran's January 8 rocket attack on U.S. military bases in Iraq clearly constituted part of its response, but Iranian leaders quickly made clear that more retaliation is forthcoming. Supreme Leader Ali Khamenei himself has said that, while the rocket attack was a "slap" at the United States, it was "not enough," and the Islamic Republic will continue its opposition to the United States with the ultimate goal of driving America out of the Middle East altogether.

Doing so, however, is likely to prove difficult for Iran. As a recent analysis by CNBC notes, sanctions leveled by the Trump administration over the past two years have inflicted extensive damage on the Iranian economy. The country's GDP shrunk by nearly 10 percent last year, and its exports of crude oil declined from a peak of 2.5 million barrels per day to less than 500,000 daily.

Domestic conditions, meanwhile, are deteriorating. Inflation is on the rise within the Islamic Republic and is now pegged at over 30 percent. So, too, is joblessness; nearly a fifth of the country's workforce is currently estimated to be unemployed. Meanwhile, governmental expenditures have surged as Iran's ayatollahs struggle to keep a lid on an increasingly impoverished, and discontented, population.

All of this, according to CNBC's analysis, profoundly limits Iran's ability "to fund a war" against the United States. But that doesn't mean the threat from Iran is nonexistent. Iran still has the ability to "ramp up its aggression against the U.S." through the use of its network of proxy forces in the region.

That network is extensive — and lethal. It comprises not only Iran's traditional terrorist proxies, such as Lebanon's Hezbollah militia and the Palestinian Hamas movement, but also assorted Shiite militias in Iraq (the so-called "Hashd al-Shaabi") and even Yemen's Houthi rebels. Recently, it has also made use of the "Shi'a Liberation Army" (SLA), a group of as many as 200,000 Shiite fighters — drawn from Afghanistan, Yemen, Pakistan, and elsewhere — that has been trained and equipped by Iran's Islamic Revolutionary Guard Corps and deployed to foreign theaters such as Syria.

Notably, these forces appear to have been thrown into chaos, at least temporarily, by the killing of Soleimani. Reports from the region suggest that Iraqi militias are "in a state of disarray" after the death of the Iranian general, and aren't currently ready to strike U.S. or allied targets. Over time, however, we can expect Tehran to regain control and direction of its troops and weaponize them anew against the United States and regional U.S. allies such as Israel, Saudi Arabia, and Bahrain. That is doubtless the top priority of Soleimani's successor as head of the Quds Force, Esmail Ghaani, who has already commenced outreach to Iranian proxies in an effort to reinforce Tehran's support for "resistance" activities.

Tehran likewise has another potent tool by which to target the United States: cyber warfare. Over the past decade, the Iranian regime has made enormous investments in its cyber-war capabilities and carried out a series of demonstration attacks on targets such as Saudi Arabia's state oil company and various U.S. financial institutions to showcase its newfound technological prowess. In the wake of President Trump's pullout from President Obama's 2015 nuclear deal, Iran reshaped its cyber-activism against the United States, focusing less on offensive attacks and more on gathering information about potential policy from the notoriously opaque new administration in Washington.

But Tehran's potential to do significant harm to the U.S. in cyberspace remains. Indeed, the U.S. Department of Homeland Security has warned publicly that Iran could carry out a cyberattack against critical U.S. infrastructure in the near future, with potentially significant "disruptive effects." And so far, neither the Pentagon nor the State Department has articulated much by way of a strategy to deter Iran from carrying out such attacks, or to mitigate the damage they could do. (In the aftermath of Soleimani's killing, that lack of strategy has become a matter of growing concern on Capitol Hill.)

Perhaps the most compelling reason to expect an asymmetric Iranian response to Soleimani's killing, however, is that asymmetric warfare plays to Iran's inherent strengths. Ever since the regime's grinding eight-year war with neighboring Iraq in the 1980s — a conflict that Iran lost handily — its leaders have exhibited a strong penchant for military asymmetry over direct confrontation. This preference has only been reinforced by persistent Western sanctions, which have eroded the country's conventional military capabilities and made the acquisition of spare parts and matériel considerably more difficult.

Soleimani was the regime's principal architect of asymmetric war, and had devoted nearly a quarter-century to building up the Islamic Republic's asymmetric potency. That is precisely why his targeted killing by the Trump administration represents such a significant blow to the integrity of Iran's proxy network — and to the prudence of its time-tested asymmetric strategy. Going forward, Tehran may well have to rethink its approach, and could conclude that the potential costs of continuing its campaign of aggression against U.S. forces in the region are now simply too high. If it doesn't, however, the very capabilities that Soleimani spent his career cultivating will remain the most potent weapons the Islamic Republic has to wield against the United States.