Exploring the Cyber Dimension of the Current U.S.-Iran Crisis

Description

Editorâ??s note: This article is part of Project Cyber, which explores modern challenges and opportunities in and through cyberspace at the intersection of irregular warfare and strategic competition. We warmly invite your participation and engagement as we embark on this project. Please submit articles here.

In the wake of the recent drone attack carried out by Iranian-backed militants, which resulted in the deaths of three U.S. servicemembers and the injury of dozens more, the Biden administration has responded with a range of actions. The most significant of these has been a series of strikes over multiple days against numerous Iranian targets and their proxies across Yemen, Syria, and Iraq. Additionally, the administration has taken non-military measures, such as economic sanctions and criminal indictments against members of the Islamic Revolutionary Guards Corps (IRGC). But there also appears to be a cyber dimension to this crisis. As administration officials debated potential response options, they reportedly considered a cyber attack. Moreover, the *New York Times* reported on Friday that cyber attacks were indeed part of the ultimate response, noting: â??Two American officials said the United States conducted cyberoperations against Iranian targets on Friday but declined to provide details.â?• Of note, also related to cyberspace, the economic sanctions the United States imposed against the IRGC included entities associated with Iranian cyber activities.

President Biden faced some vexing tradeoffs in formulating how the U.S. government would respond to the attack. On the one hand, domestic political pressure and strategic imperatives suggest a sufficiently forceful response was in order. With American lives demonstrably at riskâ??the incident represents the first time U.S. service members have been killed in the context of the ongoing conflict in the Middle Eastâ??the United States must clearly convey to Iran and its proxy groups that further violence will not be tolerated. In the context of what will invariably be a contentious and polarizing presidential election year, the Biden administration faced domestic political pressure for a strong response; Republicans called on the administration to take the fight â??to the sourceâ?• and directly attack the Iranian government. Ostensibly, the kinetic strike packages the Biden administration authorized are meant to tackle this aspect of the policy challengeâ??sending a signal of resolve to the Iranian government and its proxies to deter future attacks. The decision to use long-range bombers deployed from the U.S. homeland to strike targets in Iraq and Syria, rather than assets in the region, for instance, was likely meant to act as a signal of the range, reach, and firepower of U.S. military

capabilities.

On the other hand, the Biden administration also aims to avoid further escalating the situation and, in a worst-case scenario, unintentionally drawing the United States into a direct confrontation with Iran. How can the Biden administration square this circle? While we have little information about the cyber operations that the U.S. has reportedly conducted, academic research has shown that cyber operations during international crises, especially when they occur in tandem with other forms of signaling, can offer a way for states to take action in a manner that avoids escalationâ??a form of accommodative signaling.

This may seem counterintuitive. Cyber operations tend to be problematic when it comes to signaling resolve, especially in the context of coercive strategies. For one, they are limited in their ability to generate sufficiently high costs to deter or compel adversaries. Additionally, revealing a cyber capability to signal risks rendering it moot, undermining the inherent credibility of the signal. However, costly signals of resolve are only some of the types of signals states aim to send. For some of the same reasons that offensive cyber operations are poor tools of coercive signaling, they can be especially useful as accommodative signals during international crises.

Accommodative signals contain a mixture of resolve and reassuranceâ??they represent a Goldilocks strategy that includes coercive elements aimed at minimizing losses, and accommodative actions that demonstrate some restraint and create space for de-escalation. In the context of the current crisis, a half-measure option like an offensive cyber operation would allow the President to claim to be â??doing somethingâ?•â??in this case, applying military authorities, resources, and capabilities *directly* against the sponsor of the attack, rather than against proxy groupsâ??but in a way that carries a lower risk of escalation than kinetic attacks. Thatâ??s because offensive cyber operations have useful accommodative signaling properties. While the more sophisticated cyber attacks can cause lasting damage to networks and systems, they do not impose costs at a magnitude comparable to kinetic capabilities. Cyber attacks lack physical violence, and even the most costly forms of attack do not *directly* result in death. Moreover, the secrecy and plausible deniability associated with offensive cyber operations are useful for reassurance. Cyber operations are simply less visible to domestic audiences. In this case, they could facilitate an off-ramp to the crisis for Iranian leaders, allowing the government to absorb the attack without creating a perceived imperative to retaliate further.

U.S. officials have been reticent to share details about any purported cyber operation against Iran. Therefore, we can only speculate what form it may have taken. An offensive cyber operation that directly targets Iranian government assets is one plausible course of action. Such an operation could deny the Iranian government the ability to employ key military capabilities or systems through cyber disruption, degradation, or destruction. It would be distinct from a cyber attack against civilian critical

infrastructure (which would set a precedent the U.S. government would likely not want others to replicate). Beyond enabling the U.S. to respond to Iran itself, rather than its proxies, from a targeting perspective, it is also likely that there are far more viable cyber options against Iran. Proxy groups may have more limited infrastructure that the U.S. could target in cyberspace in a way that would net a meaningful effect.

From Iranâ??s perspective as the recipient of such signaling, these cyber operations would contrast with the highly visible and destructive kinetic attacks that have already occurred. Taken together, costly kinetic strikes aimed at Iranian interests in the region while avoiding targeting Iran directly, coupled with less costly cyber attacks, ostensibly against Iran itself, reflect a mixture of resolve and assurance. Hopefully, these measures can create a mutual faceâ??saving option for both parties to avoid further escalation.

This would not be the first time an offensive cyber operation took place in the context of a U.S.-Iran crisisâ??and did not escalate the situation. An illustrative (though imperfect) analogy to the current situation is the Trump administrationâ??s reported decision in 2019 to employ offensive cyber capabilities to retaliate against Iran. This took place in the context of a spate of Iranian attacks against oil tankers in the Strait of Hormuz and the Gulf of Oman. During that crisis, tensions ratcheted up after Iran downed a U.S. surveillance drone: U.S. and Iranian officials traded strident, blustery public statements; the U.S. authorized the deployment of an additional 10,000 troops to the region, and Iran announced that it was a few days shy of surpassing the enrichment limitations that the defunct nuclear deal had imposed. On June 21, President Trump revealed that he had approved, and then walked back, a military strike against Iran while simultaneously implying that military options were still on the table, sharing on social media: â??We were cocked & loaded to retaliate last night on 3 different sights [sic.] when I asked, how many will die. 150 people, sir, was the answer from a General. 10 minutes before the strike I stopped it.â?•

Then, media sources published reports that the U.S. government had conducted a highly tailored cyber attack against an Iranian database used to target oil tankers in the region. While the United States did not publicly claim responsibility for the cyber attack, reports relied on quotes from unnamed, current senior government officialsâ??likely a way of coupling a cyber signal with another form of communication so that the intended message is received. Such officials described the cyber operation as enabling the U.S. to â??demonstrate strengthâ?• and show that it will â??impose costs.â?• But, compared to the threat of a kinetic strike that was estimated to result in significant casualties, the offensive cyber operation was a less escalatory choice. In the current situation, the decision to couple kinetic strikes with cyber attacks rather than use the latter as a substitute for the former likely reflects the increased salience of the interests at stake.

Another aspect of the current situation that stands out from the 2019 case is the apparent decision by the Biden administration to, informally and obliquely, telegraph the potential for a retaliatory cyber attack in advance. Before the U.S. response, anonymous officials told NBC News that the U.S. would respond with a campaign that included cyber operations without specifying further details. Then, after the fact, officials confirmed that cyber operations had occurred. There are only a handful of cases where the United States has explicitly or implicitly taken responsibility for an offensive cyber operation. Examples include the 2018 operation to counter the Internet Research Agencyâ??s ability to use the Internet to interfere in the midterm elections; Operation Glowing Symphony, the cyber operation to counter the Islamic State; or cyber operations in support of Ukraineâ??s defense following Russiaâ??s 2022 invasion. Across each of these, officials have only acknowledged the role of cyber operations after the fact. This reflects the challenges described earlier of using cyber operations as a form of signaling: threatening to use a particular cyber tool against a certain target may enable defenders to take measures to identify and mitigate the threat in advance.

This is likely the first known instance of the U.S. warning of an impending cyber attack before it has taken place. While it is difficult to ascertain the motivations behind issuing an ambiguous cyber threat in advance, it does reflect a maturing appreciation of the nuances and complexities of signaling through cyber means. To wit, the implied threat was sufficiently vague to avoid communicating operational details that would undermine the feasibility of the cyber operation while also increasing the likelihood that the forthcoming cyber attack is actually perceived by the targeted and interpreted as such. Along the lines of the 2023 Department of Defense cyber strategy, applying cyber power to make adversaries â??doubt the efficacy of their military capabilitiesâ?• is more effective if that adversary observes the cyber operation in the first place and discerns its implications in the context of the ongoing crisis.

Finally, there are, of course, important limitations to offensive cyber operations. The most significant of these is that a cyber attack that will reliably cause significant effects against strategic targets is difficult to conduct and to do so with a level of reliability and precision in timing that will make it relevant. Cyber operations aimed at adversary military systems and capabilities typically depend on significant prior preparation and investment in time, resources, and skilled personnel to gain and maintain access to priority targets and develop tools that can cause the desired effects. Such accesses and exploits can be ephemeral and disappear unexpectedly. These factors will constrain the options the military is able to present to the President during a crisis. This only underscores the importance of defining clear targeting priorities in advance and directing sufficient resources to enable gaining and maintaining access to those targets so that when the President asks for a cyber course of action during a crisis or contingency, palatable options are on the table.

Erica D. Lonergan is an Assistant Professor in the School of International and Public Affairs at Columbia University. She also currently serves as a Senior Advisor to Cyberspace Solarium Commission 2.0. Previously, Erica served on the writing team of the 2023 Department of Defense Cyber Strategy and was a Senior Director on the Cyberspace Solarium Commission. She has published widely on cyber strategy and policy, including her recent Oxford University Press book, Escalation Dynamics in Cyberspace.

The views expressed are those of the author and do not reflect the official position of the United States Military Academy, Department of the Army, or Department of Defense.

Main image: Airmen from the 67th Cyberspace Wing review daily tasks at Joint Base San Antonio â?? Lacklandâ??s Medina annex, Sept. 5, 2023. The 67th Cyberspace Wing serves as the Air Forceâ??s combat cyberspace capability by presenting trained and qualified Airmen to the Cyber Mission Force. As such it acts as the serviceâ??s execution arm for generating, projecting, and sustaining global cyberspace operations. (Jason W. Edwards via U.S. Air Force)

Date Created
2024/02/13