Forecasting Iranian Government Responses to Cyberattacks

Austen Givens, PhD; Nikki Sanders; and Corye J. Douglas

Abstract: Extant scholarship on Iranian cyber warfare emphasizes the ways in which Tehran's cyber capabilities might be employed offensively to achieve its foreign policy objectives. Comparatively little attention, however, has been given to the ways in which Iran might leverage these same cyber assets in retaliatory strikes. This article argues that because of the unique combination of endogenous and exogenous variables affecting contemporary Iran, including diplomatic isolation and economic sanctions, as well as Iran's historical track record of carrying out its foreign policy through proxies, Iranian cyber retaliation is likely to be executed through third parties, mostly symbolic in nature, and proportionate in scale.

Keywords: cybersecurity, retaliation, defense, Iran, sanctions, cryptocurrency

On 3 January 2020, a missile fired from a U.S. unmanned aerial vehicle (UAV) killed Major General Qassem Soleimani, the head of Iran's Islamic Revolutionary Guard Corps (IRGC), a U.S. State Department-designated terrorist organization, at Baghdad International Airport in Iraq.[1] One of the main worries that arose in the United States within days of Soleimani's killing was that Iranian retaliation for his death would come not in the form of kinetic attacks, such as terrorist bombings, but virtually, through cyberattacks.[2] In the weeks following Soleimani's death, the U.S. De-

Dr. Austen Givens is associate professor of cybersecurity at Utica University and coauthor of *Homeland Security: An Introduction*, published in 2021 by Oxford University Press. He received a PhD in public policy from King's College London. Nikki S. Sanders is a vice president within the financial services industry and holds an MBA with a specialization in cyber policy and an undergraduate degree in business information systems. She is a writer on emerging technologies robotics/AI/ML/cryptocurrency with an emphasis on cyberspace policy and regulation. Corye J. Douglas is a writer, researcher, and risk management professional whose research has been recognized in various media outlets. He holds graduate degrees in protective management from John Jay College of Criminal Justice and cyber policy and risk analysis from Utica University.

Journal of Advanced Military Studies vol. 13, no. 1
Spring 2022
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.20221301011

partment of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) issued alerts for American businesses to be extra vigilant for the possibility of Iranian-sponsored cyber intrusions and disruptions in retaliation for Soleimani's killing.[3] Underlining the seriousness of the concern in early 2020, *Forbes* magazine published an online article just days after Soleimani's death with the title: "How To Prepare Your Business for Iranian Retaliation Cyberattacks."[4]

Analysts' apprehensions about Iranian cyber retaliation were well-founded. Tehran wields growing offensive cyber warfare capabilities, even as its conventional military forces founder from lack of experience in modern conflicts, inadequate access to new equipment, and reduced ability to participate in Joint exercises with other foreign militaries.[5] Moreover, the Islamic Republic has used its growing cyber prowess in numerous contexts, including a series of distributed denial of service (DDoS) attacks that disrupted U.S. financial institutions in 2011–13.[6]

In the end, Iran's response to Soleimani's killing fell short of analysts' worst expectations.[7] More than 20 medium-range ballistic missiles were fired from Iran into U.S. military installations across Iraq.[8] While these missiles did not kill anyone, they caused minor traumatic brain injuries in more than 100 U.S. servicemembers, likely from the concussive blasts of the missiles' impacts.[9] Moreover, two men, probably acting on behalf of the Iranian government, were indicted in Massachusetts for defacing numerous U.S.-hosted websites with anti-America, pro-Iran slogans, and images in retaliation for Soleimani's death.[10]

This article will argue that because of the unique combination of endogenous and exogenous variables squeezing Tehran, such as domestic civil unrest, global economic sanctions, and diplomatic isolation, Iran will turn increasingly to cyber warfare capabilities for military retaliation, rather than kinetic attacks. In advancing this argument, the authors contribute both to theoretical knowledge of state behavior under economic sanctions as well as empirical knowledge of Iranian military doctrine generally and its cyber warfare capabilities in particular.

In this article, "retaliation" means a belligerent act taken by one state in response to an initiating event, such as the killing of a flag officer or the imposition of a naval blockade by another state.[11] The concepts of "offensive cyber capabilities," "offensive cyber warfare," "cyberattacks," and similar formulations are used as synonyms for computer network attacks (CNAs), which refer to actions taken to disrupt, deny, degrade, or destroy information present in computer networks.[12]

There is growing interest among scholars and national security practitioners to understand how Iran's offensive cyber capabilities might be used in Iranian retaliatory strikes. Because of the delicate tensions that the United States and its allies must navigate in dealing with Iran—global financial sanctions, Tehran-backed proxy groups, and diplomatic friction, to cite three examples—cyberattacks upon Iranian networks may be increasingly preferable to kinetic attacks on physical infrastructure. For example, an adversary might choose

to disrupt public transportation systems in an Iranian city through electronic means, rather than via a missile strike, to make attack attribution difficult and reduce the prospect of Iranian retaliation.

For different reasons, such as the comparative weakness of its conventional military assets and its relative diplomatic isolation, Iran may retaliate using cyberattacks, rather than kinetic weapons. Not only does the use of cyberattacks in this regard offer Tehran a means to respond to the perceived aggression, but it also provides a way for Iran to obfuscate their origin of the response. This can help avoid an escalatory, tit-for-tat series of reprisals that might draw Iran into open conflict and jeopardize the Iranian regime.

Why Iran?

The present article's narrow focus on Iran is driven by three primary factors: scholarly interest in how Iran conducts foreign policy, Iran's specific role as an antagonist to U.S. interests, and Iran's embrace of offensive cyber warfare during the past decade.

The contemporary politics of the Middle East are complex, involving myriad historical, religious, ethnic, tribal, and economic variables, among other factors. Yet, it would be fair to say that two of the most politically influential nation-states in the region today are Iran and Saudi Arabia, a point on which there seems to be a general consensus among scholars.[13] Both nations seek to project power within the region and beyond, through conventional means, like energy exports from Saudi Arabia, or through proxies, such as Iran's support for the Lebanese group Hezbollah.[14] To understand the present political dynamics of the Middle East, then, it is indispensable for scholars to analyze Iran and how it pursues its foreign policy objectives.

In a related vein, ties between Iran and the United States have been marked by fissures and tensions since the Iranian revolution of 1979, during which the U.S. embassy in Tehran was seized by Iranian nationals and U.S. government personnel were held hostage for 444 days.[15] In the intervening decades, Iran has provided financial and materiel support to U.S. State Department-designated terrorist organizations such as Hezbollah and Hamas.[16] And, at the time of this writing, Iran and the United States are engaged in on-again, off-again negotiations concerning the future of Iran's nuclear ambitions.[17] These facts make Iran a compelling case study for scholars and national security practitioners.

Lastly, Iran has made impressive strides in developing its cyber warfare capabilities during the past decade, despite the burden of economic sanctions and diplomatic isolation. The authors explore these developments in depth below. This progress in cyber warfare matters because Iran is included among the "big four" nation-state threats to U.S. interests today, alongside North Korea, Russia, and China.[18] The U.S. Intelligence Community highlights Iran in its *Annual Threat Assessment*, for example, and suggests that explorations of Tehran's cyber prowess are needed to bolster understandings of potential Iranian actions.

Methods

The present study was carried out in three distinct phases. The first phase involved a systematic review of peer-reviewed literature on military response forecasting. Our objective in this phase of the study was to identify common themes in the military forecasting literature relevant to the authors' study. Specifically, this article's purpose was to integrate these themes into the analyses by constructing a framework specific to Iran that may also apply to predictions about other militaries' possible responses to cyberattacks. In other words, in developing a framework to forecast Iran-specific military courses of actions, the authors may also be able to shed light on the calculations other nation-states employ to decide whether to retaliate electronically.

Database searches (e.g., EBSCO and JSTOR) used combinations of terms like "military forecasting models" and "strategic studies armed force forecasting tools" to identify literature of interest published between the years 2010–20. This time frame was chosen because the authors agreed that relevant literature predating 2010, while useful, would almost certainly have been overtaken by newer scholarship on military forecasting, particularly in light of major geopolitical events that have occurred since 2010, such as the U.S. withdrawal from Iraq and the buildup of Chinese military infrastructure in the South China Sea. Articles based on a preliminary review appeared to be relevant, but ones that on closer examination were not relevant were discarded. The key criterion for including research was whether the articles discussed methods or techniques for predicting nation-state behavior, or articles that included material which, while not tied to nation-states, could nonetheless prove useful in forecasts of state behavior. After the initial search for literature that appeared relevant to the study was complete, the authors were left with 10 peer-reviewed articles that the authors examined in detail.

The second phase of the study included a systematic review of peer-reviewed literature as well as press accounts and government statements about Iranian offensive cyber capabilities and past attributed Iranian cyberattacks. The authors examined refereed journal articles, white papers from reputable think tanks, pieces from leading magazines such as *Foreign Affairs*, and industry reports from firms like FireEye. These materials were reviewed to discern the primary drivers and themes of contemporary Iranian foreign policy, including how Tehran uses its military assets—kinetic and virtual—as instruments of foreign policy. If the United States assumes that Iran's leaders are rational actors, then their uses of cyber warfare capabilities likely follow stable, predictable patterns governed by their own perceived national interests, even as those interests evolve.

The third and final phase of the study used our literature review on military forecasting and the article's evaluation of scholarship on Iranian foreign policy to develop a series of assertions about likely Iranian responses to cyberattacks on Iranian assets. By understanding how Tehran has used offensive cyber warfare capabilities to date, as well as the principal variables influencing the nation's for-

eign policy, the United States can draw inferences about how Iran would likely respond to electronic attacks.

There are significant limitations to the methods the authors have chosen to employ in this study. The array of variables that affect how any nation responds to cyberattacks is large. The closed nature of the Iranian government means that primary source documents that might be available in studies of democratic regimes' responses to cyberattacks are unavailable for the purposes of the present study. Intentional Iranian unpredictability in executing foreign policy decisions—the so-called "Madman Theory"—may also be a factor that reduces the utility and accuracy of these predictions.[19] The authors also assume that Iranian actions will follow logical, rational patterns that are consistent with Tehran's views of its own national interests. Despite these limitations, however, the authors maintain that fuller understandings of Tehran's likely responses to cyberattacks can be helpful for scholars.

The Trouble with Forecasting

The domestic political calculus of national leaders is one lens through which military responses may be forecast. Since the heads of nation-states direct their countries' armed forces, understanding how leaders decide to use their armies helps estimate foreign military intentions. In a widely cited paper on the bungled Iran hostage rescue operation that took place during the administration of U.S. president James E. "Jimmy" Carter Jr., David J. Brulé notes that leaders use a noncompensatory decision rule that heavily weights domestic political considerations above all other decision-making criteria in foreign policy.[20] Since this research directly involves a historic situation involving interactions between the U.S. and Iranian governments, the authors give it special consideration in the context of the present article. Should the use of military force endanger a leader's domestic political survival, for example, then they are unlikely to select it.

At the same time, developing correct forecasts using the noncompensatory decision rule requires near-complete knowledge of nation-states' domestic political conditions.[21] Unfortunately, no matter how robust their capabilities may be, intelligence services do not have sufficient information to understand foreign leaders' domestic political constraints fully. They lack complete knowledge of the conditions that will influence whether or not leaders elect to use force. Scholars must be careful, therefore, to ensure that their predictions about nations' uses of military force reflect holistic understandings of domestic political environments. Otherwise, those predictions will not be as helpful or accurate as they could be.

One of the earliest and most widely cited studies on forecasting military decision making appeared in the journal *Operations Research* in 1960. Douglas L. Brooks of the Massachusetts Institute of Technology argued for a novel approach to study trade-offs in military decisions by applying the methodologies

of operational research.[22] His specific areas of focus were force composition and weapons system development, which are not the subject of the present study. However, what is useful about Brooks's study for the present article are the critiques he advanced regarding forecasting methodologies. Sharpening the outlines of "fuzzy" variables in forecasting, such as the specific objectives of military forces in conflict and defining acceptable outcomes, were central to Brooks's work.[23] His study also critiques the use of economic models in forecasting military objectives, since they tend to rely on artificially constrained sets of variables and are static in nature.[24] These observations point toward the need for forecasts that capture a wide range of well-defined input variables and are sufficiently flexible to incorporate "if-then" scenarios.

An additional perspective relevant to the present study is the recognition that qualitative narratives can shape threat perceptions as well as agendas for possible courses of action. Writing in 2018, Cameron A. MacKenzie et al. argue that qualitative understandings of design requirements can be valuable for improving engineers' knowledge of how to build and design products.[25] MacKenzie et al.'s work is helpful for the present article, for history shows that narratives can alter political calculations, influencing leaders' decisions around uses of force.

Forecasts of civilian support mobilizations can also provide instructive points of reference for anticipating future uses of the armed forces. A study for the U.S. Army published in 2019 by Rand is illuminating in this regard. Tasked with anticipating how the U.S. Department of Defense might use noncombatant civilians for future overseas contingency operations, a team of researchers used a mixed-methods approach incorporating a literature review, elite interviews with key decision makers, historical analyses, linear regressions, and machine learning.[26]

While the content of the Rand study does not relate specifically to research on Iranian cyber retaliation, what the authors find compelling and relevant is the diverse mixture of methods they applied to their inquiry. The tools and techniques used to complete this study yielded robust results. Yet, while these methods help us to understand how forecasts of military behavior can be produced, the unfortunate reality is that they cannot be generated in the same manner for analyses of *foreign* militaries. After all, the data sets and decision makers to which the Rand team had access were open and accessible to the researchers, since the Department of Defense (DOD) hired Rand to produce the study. However, it is unthinkable that U.S. adversaries would grant U.S.-based researchers unfettered access to their defense personnel, weapons systems, or secure communications networks. To do so would undermine their operational security and cede strategic and tactical advantages for no perceptible benefit.

One stream of literature that would appear relevant to the present study, but which is not incorporated into this article's analyses, is game theory. In recent years, game theory scholarship has been applied to a host of problems, from network behavior to predicting clinical depression.[27] Yet, as shown earlier

in this section, forecasting future state behaviors requires incorporating a wide array of variables. Even the simplest mathematical models would still have to be simplified for analysis purposes, potentially skewing results and reducing their accuracy. In the authors' view, the noncompensatory decision rule, coupled with historical information about past Iranian behavior, offers greater explanatory power and potentially more precise predictions than game theory.

The military forecasting literature suggests that a few major variables will likely determine Iranian responses to cyberattacks. The first and most likely is the noncompensatory decision rule. The Iranian regime is concerned, above all, with its own survival.[28] Therefore, measures that the regime may undertake in response to cyberattacks, or any other crisis for that matter, will prioritize this survival. Moreover, carefully defining input variables used in forecasts is indispensable for accuracy. It is important to guard against the possibility of qualitative narratives about Iranian force strength and intentions skewing the results of analyses. Furthermore, the range of input variables used in military forecasts is broad enough to capture various possible factors that will shape military responses to cyberattacks.

The Increasing Importance of Cyber Operations in Iran

Extant scholarship on Iranian offensive cyber operations emphasizes how Iran uses these operations to gain strategic advantages over its adversaries. However, the degree to which Iran might employ these same tools and tactics to respond to cyberattacks on its own infrastructure remains underexamined by scholars.

Knowledge of Iran's development of offensive cyber warfare capabilities has grown during the past decade. Some researchers have pointed out that Iran's burgeoning interest in cyber warfare is congruent with the nation's general preference for using ambiguity, such as foreign proxy groups, to achieve its policy goals.[29] And a clear track record of Iranian cyberattacks to advance the nation's interests highlights the rising significance of offensive cyber capabilities for Iranian foreign and domestic policy.[30]

Iran has limited ability to use its own conventional military assets to project power abroad.[31] One way that Iran gets around this comparative weakness is by sponsoring and partnering with proxy groups and allied governments in the Middle East.[32] In addition, Tehran has begun to exert power in cyberspace against the United States, its allies, and domestic groups from within Iran itself.[33] It is important to underline here that the examples the authors share below do not represent all of Iran's cyberattacks, either directly or through proxies, during the past 10 years. Rather, these are among the most prominent examples of Iran-linked cyberattacks reported in the public domain.

One of Iran's first publicly attributed uses of cyber warfare during the past decade took place in a series of DDoS attacks against the U.S. financial sector from 2011–13, called Operation Ababil, which the U.S. National Security Agency interpreted as a response to Western efforts to stymie the Iranian nuclear program.[34] Campaigns linked to the Izz ad-Din al-Qassam Cyber Fighters

(QCF), a proxy group connected to the IRGC, attacked American financial institutions.[35] The origins of the DDoS attacks were by their nature ambiguous, since DDoS attacks use large networks of computers called "botnets" to attack targets, making attribution difficult. It is estimated that 50 U.S. banks, including Bank of America, were the victims of these attacks.[36] Operation Ababil shows Iran's willingness to leverage cyberspace to attack critical infrastructure. Given the constraints Iran faces, Tehran has much to gain and little to lose from attacks like those it leveled in Operation Ababil.

Other prominent examples of Iranian cyberattacks that appear offensive, rather than defensive, include data theft and destruction against a Las Vegas casino in 2014, as well as a private Iranian company that accessed the control systems for a dam in Rye, New York, in 2013.[37] While neither of these attacks caused significant damage, they illustrate that Iran can engage targets in different geographic areas and disparate economic sectors.

Shamoon, a computer virus traced to Iran that destroyed thousands of computers at Saudi-Aramco in 2012, offers an additional example of Tehran's capabilities and intentions with respect to cyber warfare.[38] Saudi-Aramco is the national petroleum company of Saudi Arabia. In addition to being petroleum exporting nations, Riyadh and Tehran are strategic rivals in the Middle East, vying for influence and power.[39] The attack resulted only in disrupted business operations, with no loss of oil production or an accidental spillage.[40] However, the signal it sent—that Iran could strike one of its rival's most essential organizations to damage infrastructure—was unmistakable.

Despite the severe effects of Operation Ababil and the Shamoon virus, scholarship also clarifies that Iranian cyber capabilities have evolved.[41] For example, one researcher highlights that the Stuxnet virus, which attacked programmable logic controllers used in the Iranian nuclear program in 2010, was initially identified by *non-Iranian* digital forensic experts. This suggests, in Max Smeets's estimation, that the Stuxnet virus was calculated not only to inflict damage on the Iranian nuclear program but to embarrass Iran. By creating a computer virus that Iranian government officials were not the first to identify publicly, the United States and Israel humiliated the Iranian regime, which was shown to be unable to protect its own clandestine nuclear program and seemingly to lack the ability to analyze malware quickly.[42] Of course, launching offensive cyberattacks (i.e., Operation Ababil) and digital forensic analyses (i.e., deconstructing Stuxnet) are different functions requiring disparate sets of skills and knowledge. However, the overall impression is that Iran's cyber prowess has grown both more sophisticated and persistent over time.[43]

Therefore, it is natural that Iran will increasingly opt to use cyberattacks in offensive (i.e., attacking first) and defensive (i.e., responding to an attack) contexts. Michael Eisenstadt even speculates that one reason Iran's preference for defensive cyberattacks will grow is that there is limited potential for spillover from the cyber to the physical domain.[44] Moreover, unlike the laws of armed conflict governing the use of kinetic weapons, there remains a good deal of am-

biguity about what acts in cyberspace may constitute acts of war.[45] Consequently, Iran can signal through cyberattacks that are more nuanced than through the use of kinetic weapons.

Some scholars express skepticism about how Iran poses a genuine threat to Western and U.S. interests. For example, Paul R. Pillar, a retired Central Intelligence Agency officer, frames Iran as a useful villain for U.S. policy makers.[46] Constance Duncombe sounds a similar note, maintaining that much of the hostility in the U.S.–Iran relationship can be traced to mutual misunderstandings borne from misrepresentations.[47]

Moreover, the idea of Iranian "retaliation" may have become outmoded. Analyses from FireEye, a prominent cybersecurity firm, suggest that Iran's use of cyber responses fits into a broader spectrum of persistent activity, including online disinformation and espionage campaigns.[48] A group of scholars affiliated with the Belfer Center for Science and International Affairs at Harvard University recently argued that the "tit-for-tat" understanding of Iranian cyber actions overlooks the evolution that has taken place in Iranian cyber capabilities.[49] They maintain that while in the past, Iran's use of cyberattacks may have been in direct response to specific events, today Iran is persistent in its use of cyber capabilities. In addition, they argue that U.S. analyses of Iranian intentions suffer from "mirror imaging"—that is, the projection of American decision-making calculus onto Iranian actors, a concern that we share about the present study.[50]

This article is agnostic with respect to the seriousness of the threat that Iran poses. Tehran's track record of cyberattacks to date suggests that it can strike a variety of targets, yet its ability to inflict damage remains limited. The authors also believe that it is possible for Iranian cyber responses to fit within a more expansive, ongoing backdrop of Iranian cyber activity. The focus of this article is neither to assess the gravity of the Iranian threat, nor to contextualize Iran's use of cyberattacks as one tool in its arsenal of online activities. Rather, the objective is to show that Iran's use of cyberattacks for retaliation is a natural outcome of the internal and external factors affecting Tehran today.

The Economic and Diplomatic Drivers of Iranian Cyber Warfare Capabilities

To understand why Tehran is investing in cyber warfare capabilities, it is helpful to examine its growing cyber prowess through the lenses of economics and diplomacy. Other possible factors, such as postrevolutionary Iranian domestic politics, help clarify Iran's embrace of cyber capabilities. However, as the article details below, economics and diplomacy offer a great deal of explanatory power in this context. And while there is a clear overlap between these two perspectives, the authors treat economics and diplomacy independently for this analysis.

In recent years, the financial restrictions imposed on Iran have stunted Iran's economy and worsened the nation's already limited ability to procure and service its conventional military assets.[51] For example, in 2013, sanctions

imposed by the Barack H. Obama administration all but halted Iran's gold and currency trading activities.[52] Tehran's access to the Society for Worldwide Interbank Financial Telecommunication (SWIFT), which undergirds the electronic global transfer of money, was cut off.[53] World Bank data shows that Iran's annual gross domestic product (GDP) has fluctuated from about -7.4 percent in 2012, to 13.396 percent in 2016, to -6.78 percent in 2019.[54] The Iranian rial depreciated 78 percent against the U.S. dollar in two months in 2018. At least some of this currency volatility is attributable to the effects of global economic sanctions imposed on the country.

Moreover, throughout much of the Donald J. Trump administration, Iran ranked in the lower two quintiles of national GDPs that the World Bank tracks.[55] Sanctions led to economic uncertainty, catalyzing massive capital flight from Iran beginning in 2018.[56] Among other effects, the sanctions have contributed to increases in the cost of living for ordinary Iranians, sharp downturns in oil exports, and they nearly halted the domestic manufacture of pharmaceuticals.[57]

However, it is important to note that the imposition of economic sanctions alone does not necessarily deter a state from pursuing certain policy outcomes.[58] Rather, as Robert A. Pape has shown, modern states are adaptable and will turn to substitutions to mitigate the effects of sanctions.[59]

And, indeed, Iran is using innovative measures to evade sanctions. Research and intelligence in the public domain reveal that Iran is amassing wealth in the form of cryptocurrency, probably to dodge the punishing effects of global economic sanctions.[60] A newly identified Iranian cyber group, Agrius, is suspected in a November 2020 series of data wiping attacks disguised as ransomware targeting U.S. allies.[61] Among other activities, the bounties from ransomware could help to fund Iran's support of terrorist organizations like Hezbollah and buttress Tehran's efforts to reengage with the global financial system.

Evidence of Iran's intent lies in the Iranian government, its central bank, and its affiliates' actions and statements.[62] For example, former Iranian president Hassan Rouhani made cryptocurrency mining a part of the state apparatus, imposing policies for cryptocurrency miners to be licensed.[63] The Iranian Ministry of Intelligence is tasked with tracing illegal cryptocurrency mining activities. In parallel with these activities, the country's central bank is charged with ensuring banks and moneychangers are leveraging licensed cryptocurrency miners in global trade transactions and preventing cryptocurrency mining outside of its borders to stymie capital flight.[64] As of August 2021, according to one source, some 30 cryptocurrency mining licenses have reportedly been issued by the Ministry of Industries, Mining, and Trade.[65]

One Iranian think tank reports the country could generate $2 million a day and $700 million a year from cryptocurrency mining, with transactions fees alone generating $22 million.[66] Cryptocurrency intelligence company CipherTrace notes that laundering cryptocurrency can potentially be used to conceal weapons purchases, train covert operatives, and cover transportation costs in-

ternationally.[67] One report on Iran's blockchain usage found that approximately 72,000 Iranian IP addresses could be geographically linked to digital wallets traced back into global banks.[68] This suggests the presence of concrete links between Iranian cryptocurrency miners and international financial institutions. If confirmed, this would violate many of the sanctions leveled against Tehran.

Under these perilous economic conditions, it is understandable that the Iranian regime might turn to offensive cyber capabilities as a means to achieve its foreign policy goals. The buildup of these capabilities requires mostly domestic spending on education, training, and infrastructure. And this domestic spending would likely not be swept up in the economic sanctions designed to deter Iranian nuclear proliferation. To illustrate this, while Iran's regular armed forces, called the Artesh, received just 12 percent of its 2019 defense budget, the IRGC, a numerically smaller force, received 29 percent.[69] These figures suggest that Iran's budgetary prioritization of the IRGC is likely connected with its desire to invest proportionally more money in nonconventional military capabilities, such as offensive cyber warfare units, than in conventional military capacity.

Iran's behavior in this regard also appears to offer evidence supporting Pape's claims about state behavior under sanctions regimes. The Islamic Republic has adapted to its circumstances in special ways: using offensive cyber warfare tactics as a means to achieve its foreign policy objectives and actively encouraging the mining and use of cryptocurrency to loosen the strictures sanctions impose.

Turning to the diplomatic context, the Trump administration made a point of strengthening the U.S. alliance with Saudi Arabia, Iran's foil in the Middle East, and facilitating the Abraham Accords, a set of agreements normalizing relations between Israel and Arab states in the Middle East and Africa.[70] The accords have driven a diplomatic wedge between Iran and many of its most powerful neighbors, such as the United Arab Emirates. In the wake of this rapprochement between Israel and much of the Arab world, the country's diplomatic isolation has become so acute that, as Ephraim Kam of Tel Aviv University puts it, "The only country that could be defined as an ally of Iran is Syria."[71]

To be sure, Iran has been isolated diplomatically for decades, dating back at least to the 1979 revolution there.[72] Furthermore, some portion of Tehran's embrace of unconventional weapons and tactics can be attributed not to the impact of the Abraham Accords, but to the passage of time and the march of technological innovation. Still, Tehran seems to understand something fundamental about offensive cyber warfare capabilities. Unlike conventional military technologies, such as aircraft or missiles, whose sales are closely monitored and regulated, cyber technologies—the chips, software applications, and networking hardware that are the sinews of cyber warfare—are not controlled in as robust a manner. Iran's costs in terms of time, money, and effort to build up an offensive cyber warfare unit are modest compared with the development of, say, nuclear weapons.[73] While kinetic weapons are physical, and therefore subject to sabotage or destruction, offensive cyber warfare relies primarily on the recruit-

ment and development of human capital. Well-trained people are needed to plan operations, write code, deploy malicious software, create fictitious online personas, and collect intelligence. What is more, the level of expertise required to plan and execute offensive cyberattacks remains significantly less than the amount of education, training, and expertise necessary to construct and deploy other nonconventional capabilities, such as nuclear weapons.

There are additional diplomatic advantages, as well. Cyberattacks can be difficult to attribute, in part because of the vast array of technologies that support anonymous action online, such as the Tor Browser and virtual private networks (VPNs). While payoffs from offensive cyberattacks can be significant in terms of strategic advantages gained, the costs of carrying out those attacks are comparatively low. Moreover, even if the digital forensic attribution of a cyberattack is successful and supported by robust analyses, the probability of Iran extraditing one of its own citizens for having carried out a cyberattack against an adversary nation is negligible. In aggregate, these factors increase the attractiveness of offensive cyberattacks as a means for the government of Iran to advance its foreign policy objectives.

And Iran has done precisely this. For example, Tehran has used cyberattacks, such as those in Operation Ababil, as a means to retaliate for perceived aggression aimed at Iran's burgeoning nuclear weapons program. Reports of Iranian cyberattacks on the Saudi oil company Aramco, Israeli water utilities, and the U.S. power grid continue to surface.[74] The Iranian advanced persistent threat (APT) group known as Charming Kitten used a combination of social engineering tactics—that is, manipulation through deception—to target individuals on LinkedIn and WhatsApp for espionage purposes.[75] The APT group created bogus profiles impersonating Iranian academics, U.S. government employees, and journalists. In these incidents, the common attack vectors were email, text message, and instant messaging in a three-pronged strategy to gain unauthorized access and steal sensitive information.[76]

Iran is also an active participant in global online disinformation campaigns and most recently leveraged this capability to sway the outcome of the 2020 U.S. presidential election.[77] A March 2021 report shared within the U.S. Intelligence Community emphasized that these influence campaigns intended to prevent the reelection of former president Donald J. Trump.[78] Technical investigations led by the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA) regarding foreign political operations during the 2020 U.S. elections revealed vulnerabilities in election websites that were exploited and attributed to Iranian IP addresses.[79] The IRGC's disinformation teams leveraged voter information extracted during these cyber-espionage operations to spread propaganda and harass voters as a part of a malicious email campaign in October 2020.[80] These three interrelated sets of actions—computer network attacks, online disinformation campaigns, and electronic espionage—underline how far Iran has come in using cyberattacks to gain strategic advantages.

How Will Iran Respond?

Thus far, the authors have shown that Iran can use offensive cyber capabilities to advance its foreign policy agenda. However, the actual effects of its attacks have been limited (e.g., Shamoon and Operation Ababil). Defense planners in Tehran seem to think carefully before retaliating, ensuring that their actions are roughly in proportion to the attacks they have absorbed. Finally, at the time of this writing, Iran is suffering from a combination of diplomatic isolation and economic crisis, suggesting that Iranian leaders will likely avoid actions that may exacerbate their effects, as this could endanger the regime's survival.

Based on the foregoing analysis, the authors make the following four assertions about the ways in which Iran is likely to respond to a cyberattack on its own assets at the present time:

1. Iran should be expected to use third-party, nongovernmental entities to respond to cyberattacks upon Iranian assets.

Tehran's favor of proxy groups makes this outcome likely. In addition, using a third party adds a layer of plausible deniability for the regime, helping to avoid engagements against the regime itself. In addition, this third-party group may initiate retaliatory actions from outside the sovereign borders of Iran, further adding to the ambiguity surrounding the origins of the response. Two possible examples of such groups include the Mabna Institute, a private group of contractors that steal data for the IRGC, and the Iranian Cyber Army, an independent organization of hackers with murky ties to the IRGC.[81]

2. Iran's response to a cyberattack will probably be symbolic, with little actual damage inflicted on targets.

The list of known cyberattacks attributed to Iran so far suggests that Tehran enjoys a far reach. However, it is not clear that the IRGC possesses the expertise to take power grids offline, contaminate drinking water supplies, or disrupt manufacturing facilities through electronic attacks. Even the compromise of the control systems of the Bowman Dam in Rye, New York, which were tied to the IRGC, did not result in actual, physical damage to equipment nor harm to human life.[82] Rather, the IRGC's track record shows a preference for symbolic actions and targets, such as the Shamoon virus deployed against Saudi-Aramco, or even the ballistic missile launches against U.S. military installations in Iraq after the death of IRGC major general Qassem Soleimani.

3. Iranian retaliation for cyberattacks is likely to be restrained and proportionate.

Since the noncompensatory decision rule applies to military decision making, the Iranian regime is not likely to take any action to jeopardize its contin-

ued grip on power. Despite the bombastic "Death to America!" rhetoric that sometimes gets aired in Iranian media outlets, the authors estimate that Tehran will offer measured responses to cyberattacks that do not rise to a level that invites further counterattacks.[83] The regime's concern for its own survival, as well as its recognition of the nation's present diplomatic and economic vulnerability, will play pivotal roles in this regard.

4. After it retaliates, Iran will continue developing and refining its cyber warfare capabilities.

The trajectory of Iran's cyber warfare program is one of clear, if uneven, growth. As the regime continues to face global scrutiny and financial sanctions for its clandestine pursuit of nuclear weapons, it would be rational for Tehran to invest continually in offensive cyber capabilities. These capabilities offer Iran potential strategic advantages in much the same way—albeit to a much less powerful degree—than nuclear weapons. And they are less expensive to develop than other kinetic weapons.

It is important to acknowledge that although the assertions above have been developed using as inclusive and comprehensive an approach as is practicable, such forecasts are not static. While certain assertions that the authors have made are grounded in historical behavior, such as Iran's preference for third party and proxy groups, other predictions could change quickly. For example, a sudden change in leadership, or a national calamity like a worsening of the COVID-19 pandemic, could significantly alter the decision calculus of Iranian leaders.

However, putting these caveats to one side, the authors maintain that, at least for now, Iranian retaliation for cyberattacks on Iranian assets is likely to be carried out by third parties, mostly symbolic, and proportionate in scale.

Conclusions and Future Directions

This article has argued that the unique combination of internal and external factors influencing Iran today, including diplomatic isolation and global financial sanctions, will lead Tehran increasingly to use cyberattacks in military retaliations rather than kinetic weapons. In advancing this argument, the authors offered predictions about how Iran will respond to cyberattacks on its own assets, while contributing to empirical knowledge of Iranian military capabilities and theoretical understandings of state behavior under sanctions regimes.

There is a growing need for additional research in this area. One natural line of inquiry to pursue would be for scholars to assess how the COVID-19 pandemic may determine Iranian uses of cyber capabilities to pursue its domestic and international policy objectives. A second area of research that is needed relates to attribution. Several incidents during the 2020 U.S. presidential campaign, such as online disinformation campaigns traced to Iran, suggest a widening of Iran's tactics in cyberspace. Forensic analyses can publicly confirm or disconfirm Iranian culpability for these acts. Furthermore, they would add to

insights into how the Islamic Republic intends to use its cyber power in future elections.

A third topic for researchers to explore concerns Iran's pursuit of digital currency. Iran may be seeking to amass wealth through a combination of ransomware attacks and independent cryptocurrency mining. Some notable Wall Street victims of Operation Ababil have announced plans to adopt blockchain technology to leverage digital currencies for payment efficiency.[84] If many U.S. financial institutions aggressively pursue blockchain-based assets such as cryptocurrency or tokens, ransomware attacks on the U.S. banking system could be attractive for Iran.

The coming years will be formative for Iran's cyber warfare capabilities. Just as domestic unrest and international pressures have helped spur the development of Iran's capacity in cyberspace to date, so too will the COVID-19 pandemic and the expanding use of cryptocurrencies affect how it chooses to retaliate in the future.

Endnotes

1. Wayne Rash, "How to Prepare Your Business for Iranian Retaliation Cyberattacks," *Forbes*, 13 January 2020; "Foreign Terrorist Organizations," U.S. Department of State, accessed 16 February 2022; and "Statement on the Killing of Qassem Soleimani," U.S. Department of Defense, 2 January 2020.
2. For examples of how academic and industry analysts predicted Iranian retaliation through cyberattacks, see Annie Fixler, "The Cyber Threat from Iran After the Death of Soleimani," *CTCSentinel* 13, no. 2 (February 2020): 20–29; and see also "Iran retaliates for the killing of Qassem Suleimani," *Economist*, 8 January 2020.
3. Fixler, "The Cyber Threat from Iran After the Death of Soleimani," 20–21, 24.
4. Rash, "How to Prepare Your Business for Iranian Retaliation Cyberattacks."
5. Rash, "How to Prepare Your Business for Iranian Retaliation Cyberattacks."
6. "International Cyber Crime: Iranians Charged with Hacking U.S. Financial Sector," Federal Bureau of Investigation, 24 March 2016.
7. For example, see, "Potential for Iranian cyber response to U.S. Military Strike in Baghdad," Cybersecurity and Infrastructure Security Agency, 6 January 2020; Fixler, "The Cyber Threat from Iran After the Death of Soleimani"; and "Iran Retaliates for the Killing of Qassem Suleimani."
8. Alissa J. Rubin et al., "Iran Fires on U.S. Forces at 2 Bases in Iraq, Calling It 'Fierce Revenge'," *New York Times*, 7 January 2020; and Idrees Ali and Phil Stewart, "More than 100 U.S. Troops Diagnosed with Brain Injuries from Iran Attack," Reuters, 10 February 2020.
9. Rubin, "Iran Fires on U.S. Forces at 2 Bases in Iraq, Calling It 'Fierce Revenge' "; and Ali and Stewart, "More than 100 U.S. Troops Diagnosed with Brain Injuries from Iran Attack."
10. United States of America v. Behzad Mohammadzadeh and Marwan Abusrour, Indictment, Criminal No. 20-cr-10182, 3 September 2020, United States District Court (District of Massachusetts), 4–7; and Gordon Lubold, Nancy A. Youssef, and Isabel Coles, "Iran Fires Missiles at U.S. Forces in Iraq," *Wall Street Journal*, 7 January 2020.
11. Françoise J. Hampson, "Belligerent Reprisals and the 1977 Protocols to the Geneva Conventions of 1949," *International and Comparative Law Quarterly* 37, no. 4 (October 1988): 820.
12. "Computer Network Attack (CNA)," National Institutes of Standards and Technology, accessed 16 February 2022.

13. For example, see generally, Martin Beck, "The Aggravated Struggle for Regional Power in the Middle East: American Allies Saudi Arabia and Israel versus Iran," *Global Policy* 11, no. 1 (February 2020): 84–92, https://doi.org/10.1111/1758-5899.12778; and Ibrahim Fraihat, *Iran and Saudi Arabia: Taming a Chaotic Conflict* (Edinburgh, Scotland: Edinburgh University Press, 2020).
14. Hezbollah is both a U.S. State Department-designated terrorist organization as well as a political party in Lebanon.
15. "The Iranian Hostage Crisis," U.S. Department of State, accessed 16 February 2022.
16. Michael Levin, "Iran, Hamas and Palestinian Islamic Jihad," Wilson Center, 21 May 2021; and Suzanne Maloney, "Major Beneficiaries of the Iran Deal: The IRGC and Hezbollah," Brookings Institution, 17 September 2015.
17. Laurence Norman, "Differences Splinter U.S. Team Negotiating with Iran on Nuclear Deal," *Wall Street Journal*, 24 January 2022.
18. See, for example, *Annual Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, 2021), 12–14.
19. For a recent and fascinating reconsideration of the "Madman Theory," see Roseanne W. McManus, "Revisiting the Madman Theory: Evaluating the Impact of Different Forms of Perceived Madness in Coercive Bargaining," *Security Studies* 28, no. 5 (2019): 979–81, https://doi.org/10.1080/09636412.2019.1662482.
20. David J. Brulé, "Explaining and Forecasting Leaders' Decisions: A Poliheuristic Analysis of the Iran Hostage Rescue Decision," *International Studies Perspectives* 6, no. 1 (February 2005): 100, https://doi.org/10.1111/j.1528-3577.2005.00196.x.
21. For a recent treatment of how intelligence collection can be used to manage risk and combat cybercrime, see Alasdair Marshall et al., "Forecasting Unknown/Unknowns by Boosting the Risk Radar within the Risk Intelligent Organisation," *International Journal of Forecasting* 35, no. 2 (April-June 2019): 654–55, https://doi.org/10.1016/j.ijforecast.2018.07.015.
22. Douglas L. Brooks, "Choice of Pay-Offs for Military Operations of the Future," *Operations Research* 8, no. 2 (March–April 1960): 159–68, https://doi.org/10.1287/opre.8.2.159.
23. Brooks, "Choice of Pay-Offs for Military Operations of the Future," 160.
24. Brooks, "Choice of Pay-Offs for Military Operations of the Future," 163.
25. Cameron A. MacKenzie, Kristy A. Bryden, and Anna A. Prisacari, "Integrating Narratives into Decision Making for Complex Systems Engineering Design Issues," *Systems Engineering* 23, no. 1 (January 2020): 69–73, https://doi.org/10.1002/sys.21507.
26. Molly Dunigan et al., *Army Expeditionary Civilian Demand: Forecasting Future Requirements for Civilian Deployments* (Santa Monica, CA: Rand Corporation, 2019), 6, https://doi.org/10.7249/RR2854.
27. For example, see Rodica Ioana Lung, Camelia Chira, and Anca Andreica, "Game Theory and Extremal Optimization for Community Detection in Complex Dynamic Networks," *PLOS One* 9, no. 2 (February 2014): 1–11, https://doi.org/10.1371/journal.pone.0086891; see also R. Loula and L. H. A. Monteiro, "A Game Theory-Based Model for Predicting Depression Due to Frustration in Competitive Environments," *Computational and Mathematical Methods in Medicine* (June 2020): 1–6, https://doi.org/10.1155/2020/3573267.
28. *Iran Military Power: Ensuring Regime Survival and Security Regional Dominance* (Washington, DC: Defense Intelligence Agency, 2019), 15.
29. Michael Eisenstadt, "Iran's Lengthening Cyber Shadow," Washington Institute for Near East Policy, Research Notes no. 34, 28 July 2016, 1; and Michael Connell, "Iran's Military Doctrine," United States Institute of Peace, 11 October 2010.
30. Eisenstadt, "Iran's Lengthening Cyber Shadow," 1; and Monica Kaminska, "Restraint Under Conditions of Uncertainty: Why the United States Tolerates Cyberattacks," *Journal of Cybersecurity* 7, no. 1 (2021): 2, 9, https://doi.org/10.1093/cybsec/tyab008.
31. *Iran Military Power*, 15.
32. *Iran Military Power*, 15.
33. Julia Voo et al., *National Cyber Power Index 2020: Methodology and Analytical Consid-*

erations (Cambridge, MA: Harvard Kennedy School, Belfer Center for Science and International Affairs, 2020), 14–15.

34. Kaminska, "Restraint Under Conditions of Uncertainty," 2, 9.
35. Jamie Collier, "Proxy Actors in the Cyber Domain: Implications for State Strategy," *Antony's International Review* 13, no. 1 (May 2017): 25–47; "Iranian DDoS Attacks: Conspiracy to Commit Computer Intrusion," Federal Bureau of Investigation, accessed 17 February 2022; Dustin Volz and Jim Finkle, "U.S. Indicts Iranians for Hacking Dozens of Banks, New York Dam," Reuters, 25 March 2016; and "Denial of Service Attacks against U.S. Banks in 2012–2013," Council on Foreign Relations, September 2012.
36. "Denial of Service Attacks against U.S. Banks in 2012–2013."
37. "Denial of Service Attacks against U.S. Banks in 2012–2013," 2.
38. Max Smeets, "The Strategic Promise of Offensive Cyber Operations," *Strategic Studies Quarterly* 12, no. 3 (Fall 2018): 93; and Eisenstadt, "Iran's Lengthening Cyber Shadow," 3.
39. See generally, "Managing the Saudi-Iran Rivalry," Council on Foreign Relations, 25 October 2016.
40. Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *New York Times*, 23 October 2012.
41. James Shires and Michael McGetrick, *Rational Not Reactive: Re-evaluating Iranian Cyber Strategy* (Cambridge, MA: Harvard Kennedy School, Belfer Center for Science and International Affairs, October 2021), vii.
42. Smeets, "The Strategic Promise of Offensive Cyber Operations," 102.
43. Shires and McGetrick, *Rational Not Reactive*, 8.
44. Eisenstadt, "Iran's Lengthening Cyber Shadow," 12.
45. Eisenstadt, "Iran's Lengthening Cyber Shadow," 12.
46. Paul R. Pillar, "The Role of Villain: Iran and U.S. Foreign Policy," *Political Science Quarterly* 131, no. 2 (Summer 2016): 367, https://doi.org/10.1002/polq.12479.
47. Constance Duncombe, "Representation, Recognition and Foreign Policy in the Iran-US Relationship," *European Journal of International Relations* 22, no. 3 (2016): 622–45, https://doi.org/10.1177/1354066115597049.
48. For example, see *Suspected Iranian Influence Operation: Leveraging Inauthentic News Sites and Social Media Aimed at U.S., U.K, Other Audiences* (Milpitas, CA: FireEye, 2018); and Jacqueline O'Leary et al., "Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and Has Ties to Destructive Malware," *FireEye Threat Research Blog*, 20 September 2017.
49. See, generally, Shires and McGetrick, *Rational Not Reactive*.
50. Shires and McGetrick, *Rational Not Reactive,* 29–31.
51. Hadi Ajili and Mahsa Rouhi, "Iran's Military Strategy," *Survival: Global Politics and Strategy* 61, no. 6 (November 2019): 139–52, https://doi.org/10.1080/00396338.2019.1688575.
52. Mahmood Monshipouri and Manochehr Dorraj, "Iran's Foreign Policy: A Shifting Strategic Landscape," *Middle East Policy* 20, no. 4 (Winter 2013): 136, https://doi.org/10.1111/mepo.12052.
53. Monshipouri and Dorraj, "Iran's Foreign Policy," 136.
54. "GDP Growth (Annual %)—Iran, Islamic Rep. (Line Graph, 1961–2020)," World Bank, accessed 17 February 2022.
55. "GDP Growth (Annual %)—Iran, Islamic. Rep (Global Heat Map, 2020)."
56. Pooya Azadi, *Governance Deadlock and Economic Crisis in Iran* (Redwood City, CA: Stanford University Iran 2040 Project, 2021), 2.
57. "Six Charts that Show How Hard US Sanctions Have Hit Iran," BBC, 9 December 2019.
58. Robert A. Pape, "Why Economic Sanctions Do Not Work," *International Security* 22, no. 2 (Fall 1997): 93, https://doi.org/10.2307/2539368.
59. Pape, "Why Economic Sanctions Do Not Work," 93.
60. For example, see Tom Robinson, "How Iran Uses Bitcoin Mining to Evade Sanctions

and 'Export' Millions of Barrels of Oil," *Elliptic* (blog), 21 May 2021; and "Iran Uses Crypto Mining to Lessen Impact of Sanctions, Study Finds," Reuters, 21 May 2021.

61. Amitai Ben Shushan Ehrlich, *From Wiper to Ransomware: The Evolution of Agrius* (Mountain View, CA: Sentinel Labs Research Team, May 2021).
62. Robinson, "How Iran Uses Bitcoing Mining to Evade Sanctions and 'Export' Millions of Barrels of Oil."
63. Sebastian Sinclair, "Iran's Ministry of Industry Issues 30 Licenses to Crypto Mining Farms," CoinDesk, 27 June 2021.
64. "Iran Uses Crypto Mining to Lessen Impact of Sanctions, Study Finds," Reuters, 21 May 2021.
65. Lubomir Tassev, "Iran Counts 30 Crypto Mining Farms Licensed to Mint Digital Currencies," Bitcoin.com, 26 June 2021.
66. Behnam Gholipour, "Official Report: Iran Could Use Cryptocurrencies to Avoid Sanctions," IranWire, 2 March 2020.
67. See generally, *Cryptocurrency Crime and Anti-Money Laundering Report* (Menlo Park, CA: CipherTrace, 2021).
68. Dave Jevans, "Sanctions Research: More than 72,000 Unique Iranian IP Addresses Linked to More than 4.5 Million Unique Bitcoin Addresses," CipherTrace, 17 May 2021.
69. *Iran Military Power: Ensuring Regime Survival and Security Regional Dominance* (Washington, DC: Defense Intelligence Agency, 2019), 18.
70. "The Abraham Accords Declarations," U.S. Department of State, accessed 22 March 2022.
71. Ephraim Kam, "Iran-Russia-Syria: A Threefold Cord Is Not Quickly Broken," in *Iran in a Changing Strategic Environment*, ed. Meir Litvak, Emily B. Landau, and Ephraim Kam (Tel Aviv, Israel: Institute for National Security Studies at Tel Aviv University, 2018), 33.
72. Semira N. Nikou, "Timeline of Iran's Foreign Relations," U.S. Institute of Peace, 10 August 2021.
73. *Iran Military Power*, 35–36.
74. Christopher Bronk and Eneken Tikk-Ringas, "The Cyber Attack on Saudi Aramco," *Survival* 55, no. 2 (2013): 81–96, https://doi.org/10.1080/00396338.2013.78446; Joby Warrick and Ellen Nakashima, "Foreign Intelligence Officials Say Attempted Cyberattack on Israeli Water Utilities Linked to Iran," *Washington Post*, 5 August 2020; Robert K. Knake, *A Cyberattack on the U.S. Power Grid* (Washington, DC: Council on Foreign Relations, 2017); and Frederick W. Kagan and Tommy Stiansen, *The Growing Cyberthreat from Iran: The Initial Report of Project Pistachio Harvest* (Washington, DC: American Enterprise Institute Critical Threats Project and Norse Corporation, 2015).
75. An *advanced persistent threat* (APT) is a group of information technology experts that is capable of penetrating and obfuscating their presence within secure computer networks and systems, without authorization, for extended periods of time. APTs are usually tied to nation-states' governments, but they are designed to provide a veneer of plausible deniability for their controllers. For example, see Tara Seals, "Charming Kitten Returns with WhatsApp, LinkedIn Effort," Threat Post, 31 August 2020.
76. *The Kittens Are Back in Town 3: Charming Kitten Campaign Evolved and Deploying Spear-Phishing link by WhatsApp* (Tel Aviv, Israel: ClearSky Cyber Security, 2020), 7–17.
77. "United States Seizes Domain Names Used by Iran's Islamic Revolutionary Guard Corps," U.S. Department of Justice, 7 October 2020.
78. "Government Agencies and Private Companies Undertake Actions to Limit the Impact of Foreign Influence and Interference in the 2020 U.S. Election," *American Journal of International Law* 115, no. 2 (2021): 316, https://doi.org/10.1017/ajil.2021.10.
79. "Iranian Advanced Persistent Threat Actors Threaten Election-Related Systems," Cybersecurity and Infrastructure Security Agency, 22 October 2020.
80. Erik Tucker and Frank Bajak, "U.S. Officials Link Iran to Emails Meant to Intimidate Voters," Associated Press, 21 October 2020.

81. Catherine A. Theohary, *Iranian Offensive Cyberattack Capabilities* (Washington, DC: Congressional Research Service, 2020), 1–2.
82. Joseph Berger, "A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case," *New York Times*, 5 March 2016.
83. Calvin Woodward and Jon Gambrell, "AP Fact Check: 'Death to America' Chants Live on in Iran," Associated Press, 14 June 2019.
84. "J.P. Morgan Creates Digital Coin for Payments," J. P. Morgan, 1 February 2021.