CYBER PROJECT

Rational Not Reactive

Re-evaluating Iranian Cyber Strategy

James Shires, Michael McGetrick
Foreword by Lauren Zabierek, Cyber Project

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
OCTOBER 2021

Cyber Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/Cyber

CYBER PROJECT

Rational Not Reactive

Re-evaluating Iranian Cyber Strategy

James Shires, Michael McGetrick
Foreword by Lauren Zabierek, Cyber Project

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
OCTOBER 2021

About the Authors

James Shires is an Assistant Professor in Cybersecurity Governance at the Institute of Security and Global Affairs, University of Leiden. He is a research fellow with The Hague Program for Cyber Norms and the Cyber Statecraft Initiative at the Atlantic Council, and was formerly a post-doctoral fellow with the Belfer Center's Cyber Project and Middle East Initiative. He is the author of *The Politics of Cybersecurity in the Middle East* (Hurst/Oxford University Press, 2021), and has written widely on issues of cybersecurity and international politics. A full list of publications is available at jamesshires.com, and he can be reached on Twitter @jamessshires.

Michael McGetrick is a joint MBA-MPP student currently enrolled at MIT's Sloan School of Management. Prior to his time at Harvard and MIT, he served as a submarine officer in the Navy. His active duty time consisted of a variety of nuclear power training schools, three years onboard a Los Angeles Class fast-attack submarine, and a tour as a congressional liaison. While onboard the submarine, Mike deployed to the Western Pacific twice and participated in a variety of bilateral and multinational exercises. He also earned a Master's degree from the U.S. Naval War College in Defense and Strategic Studies with a concentration in the Asia-Pacific region while serving in Washington, DC.

About the Cyber Project

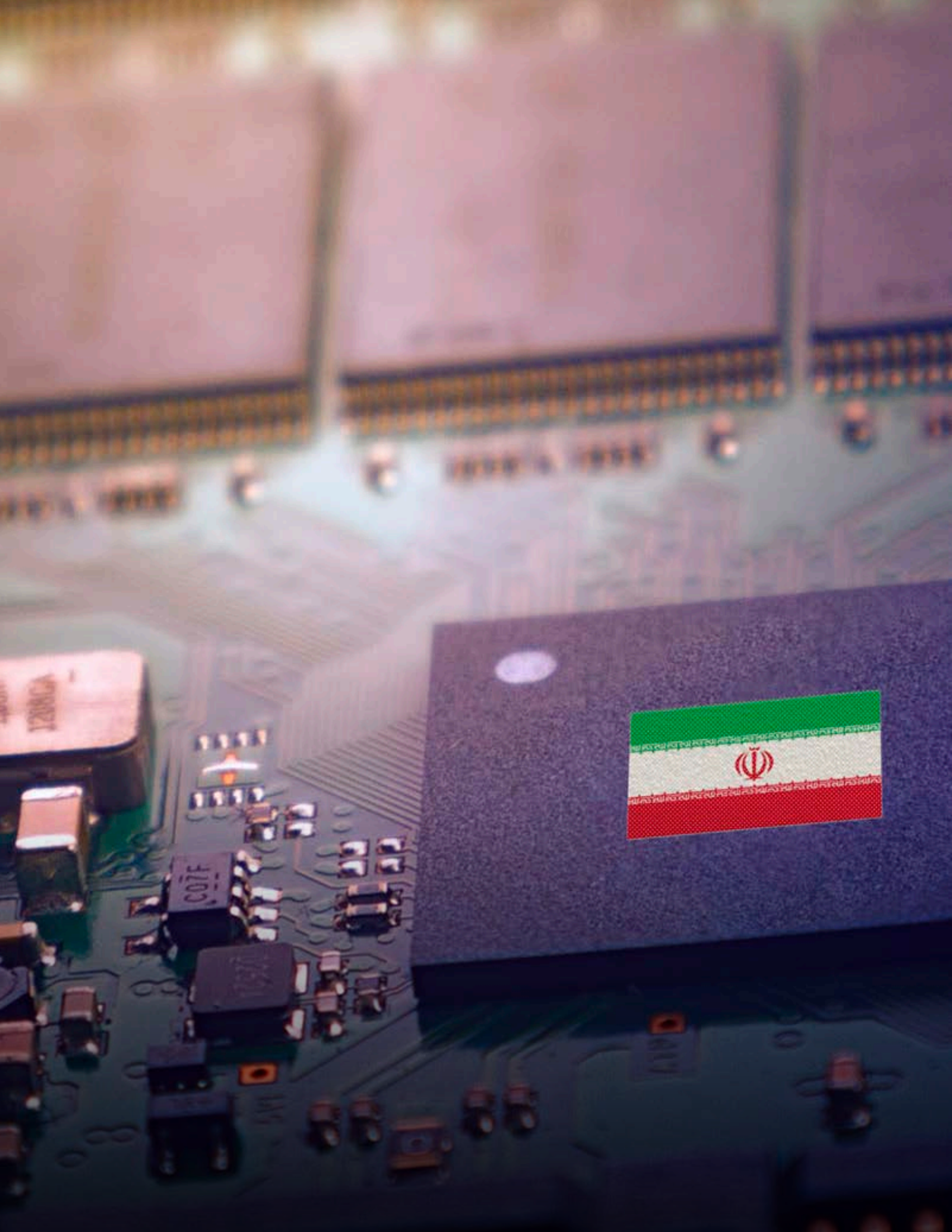
Forty years ago, an interdisciplinary group of Harvard scholars—professors, researchers and practitioners—came together to tackle the greatest threat of the Cold War: the fear of a nuclear exchange between the Soviet Union and the United States. Today, the Cyber Project seek to recreate that interdisciplinary approach to tackle a new threat: the risk of conflict in cyberspace.

The problems that confront today's leaders are substantial and diverse: how to protect a nation's most critical infrastructure from cyber attack; how to organize, train, and equip a military force to prevail in the event of future conflict in cyberspace; how to deter nation-state and terrorist adversaries from conducting attacks in cyberspace; how to control escalation in the event of a conflict in cyberspace; and how to leverage legal and policy instruments to reduce the national attack surface without stifling innovation. These are just a sample of the motivating questions that drive our work. The aim of the Belfer Center's Cyber Project is to become the premier home for rigorous and policy-relevant study of these and related questions.

Acknowledgments

The authors are extremely grateful to Usha Sahay, who contributed extensively to the research for this paper during her time as a Belfer Center student fellow, and Selena Larson for her insightful comments in a review of an earlier version of this paper. Thank you both for your time and expertise—all remaining errors are ours. This paper addresses several issues developed more extensively in James Shires' forthcoming book, *The Politics of Cybersecurity in the Middle East* (Hurst/Oxford University Press, 2021), although it makes a substantially different argument. Thanks to the Kuwait Program at Harvard Kennedy School's Middle East Initiative for their support of this project.

Table of Contents



Foreword

In January 2020, after the United States killed Iranian Revolutionary Guard Quds Force Commander Qassem Suleimani, I wrote a piece for the Boston Globe that predicted the conflict would continue to play out in cyberspace. While the article acknowledged that Iran declared an end to its physical retaliation for the killing, it failed to put that moment into broader strategic context.

As we now know, no retaliatory cyber activities perpetrated by Iran materialized in the immediate aftermath of those events. Based on the work of James Shires, Usha Sahay, and Michael McGetrick, we begin to understand why. I, like much of our community, had viewed Iranian cyber operations through the lens of history, where retaliation over even seemingly innocuous statements seemed to be a driver of its activities, perpetuating the idea that Iran was not a rational actor. Over time, however, the motives changed, and cyber operations appear to have become embedded into a larger strategy. But we missed that evolution, likely due to the noise surrounding the withdrawal from the JCPOA and other diplomatic and military encounters between our nations.

Indeed, from this work we can begin to understand that Iranian cyber operations are broadly focused on espionage, suppression of political opposition, and information operations.

Iran is a formidable cyber adversary and a rational actor in global geopolitics. I hope readers of this paper come away with an understanding of Iran's broader strategic goals and its use of cyber therein, as well as how the nation may view U.S. cyber activities, thus helping to avoid miscalculation and escalation. This paper can help policymakers to reframe the conversation and craft stronger policy options as we seek to rebuild any amount of trust in the hopes of renewing dialogues on nuclear issues.

Much like we've advocated for increased dialogue with China and Russia on cyber issues, there is more work to be done to understand Iranian perspectives in the cyber domain. Based on their work in the United Nations,

we know Iran has some stake in the cyber norms discussion and we would be remiss not to engage. If the Biden Administration wants to shape the conversation around cyber and jumpstart negotiations with Iran on nuclear ambitions, this may be a good place to start, especially on the Track 2 diplomatic level.

We hope you enjoy this discussion and look forward to your feedback.

—Lauren Zabierek, Executive Director of the Belfer Center's Cyber Project

Executive Summary

The increasing tempo of offensive cyber operations by Iran and its adversaries, including the U.S. and Israel, has led many commentators to label them as "tit-for-tat": a cyclical action-reaction dynamic where each side seeks to respond appropriately to an earlier violation by the other. However, this interpretation has significant theoretical and empirical deficiencies. Why, then, does a tit-for-tat narrative dominate our understanding of Iranian cyber activity, and what are the consequences?

This paper revisits the longer-term arc of Iranian cyber operations, as well as examining a key "negative" case of the aftermath of the U.S. killing of IRGC General Qassem Suleimani in January 2020, where relevant expert and policy communities expected an Iranian cyber response that was not forthcoming. It argues that unfulfilled U.S. expectations of Iranian cyber responses can be explained by two key factors.

First, these expectations stem from the framing power of historic incidents that do not reflect current operational dynamics. Early cyber operations attributed to Iran, some nearly a decade ago, perpetuate an outdated perception that Iranian cyber actors are responsive, unpredictable, and even irrational, despite extensive changes to the strategic landscape and Iranian cyber capabilities in the intervening period. While the decision to emphasize such historic incidents may be well motivated—in order to highlight risks to skeptical audiences, or to stand in for more current threat intelligence that cannot be disclosed—it leads to an inaccurate analysis of current tensions. For Iran, the strategic benefit from worldwide espionage and disinformation, along with sporadic regional disruption, likely outweighs the advantage gained from a briefly impactful but difficult-to-control and reputationally awkward U.S.-targeted operation.

Second, U.S. analyses of Iranian cyber operations can be mirror-imaging: projecting the U.S. posture onto Iranian actors, especially during Gulf tensions in 2019. During these tensions, many policy and media commentators argued that Iran could use cyber operations to retaliate while avoiding further escalation in an already highly inflammatory situation. However,

it was U.S. strategy—especially in the administration of President Donald J. Trump—that viewed offensive cyber operations as the most appropriate retaliatory tool in such situations. This U.S. shift, from prioritizing legal measures and defensive actions toward explicit acknowledgment of its own retaliatory cyber operations, made it tempting to believe Iranian decision-makers think in the same way. Instead, Iranian cyber operations focus on widespread efforts to obtain intelligence, spread supportive narratives, and suppress political opposition, punctuated by more disruptive events that are precisely *not* clearly tied to specific prior events.

Why does this matter? Thinking in terms of tit-for-tat leads to important policy miscalculations: namely, expecting disruptive Iranian cyber operations that never materialize. In the context of the new Iranian President and ongoing nuclear negotiations, presenting an accurate picture of Iranian cyber activity is vital to prevent cyber operations becoming part of unwanted escalatory cycles in the region. This conclusion has one key caveat: because it is based only on publicly available data, this study omits incidents or operations that occur but are not publicly reported, as well as operations that are detected and mitigated in their early stages before becoming a publicly reported incident.

The five policy recommendations that conclude this paper seek to help avoid future miscalculations. There are already examples of good practice, including the care of some actors to avoid associating regional cyber incidents with the Suleimani killing in early 2020. The overall goal is to view Iranian actors as rational participants in geopolitical cyber competition, rather than reactive and often irrational adversaries, taking our understanding of Iranian cyber strategy beyond tit-for-tat.

Introduction

On April 11, 2021, a blackout was reported at Iran's uranium enrichment facility in Natanz. International media quickly attributed the blast to Israeli sabotage, assisted by unusually open discussion in Israeli media outlets—albeit from anonymous sources.[1] As with previous explosions at Natanz and other military and strategic facilities in Iran since the infamous Stuxnet malware, discovered in 2010 and widely assumed to have been conducted by the U.S. and Israel, the question of whether a cyberattack was to blame soon took center stage.[2] This assessment eventually fell from favor, as reports of extensive damage and a possible insider suggested more conventional methods.[3] Even so, the possibility of a cyber operation was central to the official Iranian response, as the head of civil defense emphasized on state TV that "responding to cyberattacks is part of the country's defense might. If it is proven that our country has been targeted by a cyberattack, we will respond."[4]

Although accounts of this particular disruption later retreated from a cyber connection, it was a reasonable hypothesis given recent events. As discussed further below, the U.S. publicly acknowledged two cyberattacks against Iran during shipping tensions in 2019, Israel was linked to a cyberattack on an Iranian port in May 2020, and further cyber incidents with no firm attribution have occurred in Iran repeatedly over the last few years. The public record is equally congested on the Iranian side of the card, with many deployments of "wiping" malware in the Gulf states in the same

1 Kim Zetter, "Israel May Have Destroyed Iranian Centrifuges Simply by Cutting Power," The Intercept, April 13, 2021, https://theintercept.com/2021/04/13/iran-nuclear-natanz-israel/; Yonah Jeremy Bob, Lahav Harkov, and Tzvi Joffre, "'Mossad behind Attack on Iran's Natanz Nuclear Facility,'" *Jerusalem Post*, April 13, 2021, https://www.jpost.com/middle-east/incident-reported-in-iranian-natanz-nuclear-facility-664792.

2 Bob et al, above. For previous operations, see e.g., David E. Sanger, Eric Schmitt, and Ronen Bergman, "Long-Planned and Bigger Than Thought: Strike on Iran's Nuclear Program," *New York Times*, July 10, 2020, https://www.nytimes.com/2020/07/10/world/middleeast/iran-nuclear-trump.html. This is a common theme: the most recent example at the time of writing is Patrick Sykes, "Iran's Rail Network Hit by Possible Cyber Attack, State TV Says," *Bloomberg.Com*, July 9, 2021, https://www.bloomberg.com/news/articles/2021-07-09/iran-s-rail-network-hit-by-possible-cyber-attack-state-tv-says.

3 Staff Report, "Iran Identifies Suspect behind Blast at Natanz Nuclear Site," Reuters, April 17, 2021, https://www.reuters.com/world/middle-east/iran-state-tv-identifies-man-it-says-was-behind-blast-natanz-nuclear-site-2021-04-17/.

4 Staff Report, "Iran Threatens Retaliation after What It Calls Possible Cyber Attack on Nuclear Site," Reuters, July 4, 2020, https://www.reuters.com/article/us-iran-nuclear-natanz-idUSKBN2441VY.

period, as well as reported—but not especially sophisticated—interference with internet-connected Israeli water infrastructure.[5]

Why does a tit-for-tat narrative continue to be the dominant frame for understanding Iranian cyber activity . . . ?

This increasing tempo of public incidents, along with official comments like those above, has led many commentators to label them as "tit-for-tat": a cyclical action-reaction dynamic where each side seeks to respond "appropriately" to an earlier violation by the other. While previous scholarship has sought to move beyond a dyadic and discrete view of offensive cyber operations,[6] the tit-for-tat narrative nonetheless persists in industry, policy, and media coverage.

This paper therefore asks: why does a tit-for-tat narrative continue to be the dominant frame for understanding Iranian cyber activity, despite its theoretical deficiencies? The answer, in short, is that expectations of Iranian cyber responses are driven by the framing power of historic incidents that do not reflect the dynamics of current operational activity, along with a concurrent but opposite shift in U.S. posture toward a more assertive—and, in some cases, explicitly reactive—use of cyber operations. A combination of legacy frames and mirror-imaging leads U.S. analysts to expect Iranian cyber responses that do not occur.

To make this argument, this paper revisits the longer-term arc of Iranian cyber operations, as well as investigating what we call "negative" cases: instances where relevant expert and policy communities expected an Iranian cyber response that was not forthcoming. Looking in detail at a key negative case—the aftermath of the killing of Iranian Islamic Revolutionary Guards Corps (IRGC) General Qassem Suleimani by the U.S. in Iraq in January 2020—reveals the range of domestic, regional, and international

5 On water infrastructure, see J.D. Work and Richard J. Harknett, "Troubled Vision: Understanding Recent Israeli-Iranian Offensive Cyber Exchanges," Issue Brief (Washington, D.C: Atlantic Council, July 2020). Iran routinely denies all allegations of cyber operations. For a recent example, see the claim that such attributions are "merely politically motivated" by the current ambassador to the UN. Staff Report, "Tehran Says Ready to Aid UN to Confront Cyberattacks," *Tehran Times*, June 30, 2021, https://www.tehrantimes.com/news/462639/Tehran-says-ready-to-aid-UN-to-confront-cyberattacks.

6 Offensive cyber operations can be defined broadly as the adversarial manipulation of digital services or networks. In the terminology of the United States military, offensive cyber operations aim to disrupt, degrade, or destroy the targeted network or connected systems, or to deceive or deny adversaries access to that network or connected systems (the 5 Ds).

considerations at play in Iranian decision-making, making simple tit-for-tat calculations implausible.

The paper is structured in four sections. The first section reviews current scholarship on cyber strategy and Iranian foreign policy, highlighting both why tit-for-tat narratives are attractive and the reasons they have been rejected by recent works. The second section takes a long-term perspective on Iranian cyber operations, using several public databases of cyber operations, as well as U.S. federal indictments of Iranian cyber actors and other sources, to show that recent Iranian cyber operations are not "responses" in any meaningful sense. The third section investigates the killing of Qassem Suleimani, examining both expectations of an Iranian cyber response and why such expectations were not fulfilled. The fourth section concludes with recommendations for U.S. cybersecurity communities across public and private sectors.

1. Insights from Cyber Strategy and Iranian Foreign Policy

The disruptive potential of offensive cyber capabilities has generated widespread concern about their use for decades, and this concern has been increasingly borne out by the empirical record in recent years. Although many states have begun to develop such capabilities, Iran is one of four main state cyber threats frequently identified by the U.S. and its allies, along with Russia, China, and North Korea. Three of these four states, with the exception of China, have used cyber operations to disrupt key parts of the global economy, liberal societies and democratic processes: from manipulation of the international banking system to the infamous WannaCry and NotPetya malware, both developed using vulnerabilities allegedly leaked from the U.S. NSA, and from hack-and-leaks targeting election campaigns, anti-doping agencies, and entertainment companies to operations seeking to shut down energy networks in Ukraine.[7] The worldwide growth of cyber capabilities raises questions of cyber tactics and strategy: why do states use cyber capabilities, and what do they seek to achieve? Although the attribution of offensive cyber operations is itself a difficult investigative task and challenging policy conundrum, these questions go beyond attribution toward broader dynamics of the environment itself.

As we explore in more detail in the following section, early Iranian cyber activity quickly developed a reputation as reactive, both to cyber operations and other diplomatic actions, leading to the tit-for-tat narrative analyzed throughout this paper. In general, a tit-for-tat narrative has several advantages. Its focus on reciprocity is simple and easy to understand, with strong

7 For a good overview including the alleged NSA leaks, see Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, Massachusetts: Harvard University Press, 2020). The exception of China here excludes the long-term cumulative impact of Chinese cyber-espionage activity on the global economy, and acknowledges reports of historic China-attributed critical infrastructure intrusions that were assessed to be designed to "hold U.S. pipeline infrastructure at risk"—even if this was the intention, such capabilities have not yet been deployed for disruption. See Cybersecurity & Infrastructure Security Agency (CISA). "Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013," July 20, 2021, https://us-cert.cisa.gov/ncas/alerts/aa21-201a, and on the impact of Chinese cyber-espionage, Gilli, Andrea, and Mauro Gilli. "Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage." *International Security* 43, no. 3 (February 1, 2019): 141–89. https://doi.org/10.1162/isec_a_00337.

conceptual roots and clear offline parallels.[8] As a cyclical framework, it usefully incorporates the potential for overreaction, highlighting the risk of escalation through misperception or miscalculation.[9] It highlights that all sides seek to respond as strongly as possible without triggering escalation, depending on their tolerance for error, risk appetite, and other factors.[10] Whether escalation risks are higher in relation to cyber operations than in other arenas remains a matter of debate, due to the relative lack of control over indirect effects, and a still-developing set of international norms and doctrine around equivalence in terms of harms and targets.[11]

A tit-for-tat narrative . . . focus on reciprocity is simple and easy to understand.

A tit-for-tat narrative also encourages a cross-domain analysis, rather than seeing events "in cyberspace" as separate to conventional sabotage operations against maritime, energy, and other targets.[12] As scholars of cross-domain deterrence emphasize, cyber capabilities are only one of a range of options states can draw on to craft appropriate responses, and so reciprocity in terms of effect does not necessarily mean equivalence in terms of means.[13] When and how the effects of cyber operations are (perceived as) commensurate to their kinetic "equivalents" is an active and important area of research, and cyber operations are often seen as qualitatively different in cross-domain settings.[14]

---

8 The classic in the field (and the origin of the use of the phrase in political science) is Robert Axelrod, *The Evolution of Cooperation* (New York, NY: Basic Books, 1984). In contrast to Axelrod and most game-theoretic approaches to IR, we use the phrase "tit-for-tat" to refer to a narrative—an interpretation of events by observers—rather than a strategy that is (or should be) adopted by the actors observed. Hidemi Suganami, "Narrative Explanation and International Relations: Back to Basics," *Millennium* 37, no. 2 (December 1, 2008): 327–56.

9 The classic here is Robert Jervis, *Perception and Misperception in International Politics* (Princeton, New Jersey: Princeton University Press, 1976).

10 For such calculations in the Iranian context, see James Andrew Lewis, "Iran and Cyber Power" (Washington, D.C: Center for Strategic and International Studies (CSIS), June 25, 2019), https://www.csis.org/analysis/iran-and-cyber-power.

11 For an overview, see Benjamin Jensen and Brandon Valeriano, "What Do We Know about Cyber Escalation? Observations from Simulations and Surveys," *Issue Brief* (Washington, D.C: Atlantic Council Cyber Statecraft Initiative, November 2019).

12 Chris Demchak and Peter Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* 5, no. 1 (2011): 32–61; Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (October 1, 2013): 41–73.

13 Erik Gartzke and Jon R. Lindsay, eds., *Cross-Domain Deterrence: Strategy in an Era of Complexity* (New York, NY: Oxford University Press, 2019).

14 Sarah Kreps and Jacquelyn Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving beyond Effects-Based Logics," *Journal of Cybersecurity* 5, no. 1 (January 1, 2019), https://doi.org/10.1093/cybsec/tyz007.

However, it is worth noting that a tit-for-tat narrative has not developed around the other three major U.S. adversaries. Of these four states, Iran is exceptional in being both a prominent victim, as well as perpetrator, of offensive cyber operations. Notwithstanding the extensive digital intelligence gathering methods developed by the U.S. and its Five Eyes allies, none of the other three states has been publicly targeted by U.S. or allied offensive cyber operations to the same extent.[15] It is clear—to U.S. observers at least—that these three other states raised the level of impact, recklessness, or disruption of offensive cyber operations, while the U.S. has not (publicly) responded in kind.

A tit-for-tat narrative brackets contested justifications (for cyber operations), especially in relation to monitoring and countering the Iranian nuclear program.

In contrast, by understanding offensive cyber operations against Iran, as well as Iran's responses, as part of a reactive cycle with no agreed point of initiation, the tit-for-tat narrative brackets contested justifications for such operations, especially in relation to monitoring and countering the Iranian nuclear program. There have been extensive debates around the technical precision of the Stuxnet malware in the decade since it was revealed, especially on the influence of legal constraints and broader concerns around proportionality in its development.[16] Even so, the influence of Stuxnet and related wiping malware in the early development of Iranian cyber capabilities means that a simple portrayal of Iran as unprovoked cyber aggressor, along the lines of the three other states above, is implausible. In an initial comparative perspective, then, we can immediately see the uniqueness (and utility) of the tit-for-tat narrative around Iran for U.S. observers. It takes for granted—or, more strongly, *naturalizes*—the use of offensive cyber operations against Iran, avoiding difficult questions about the U.S. role that arise, if they do so at all, in a very different way for the other three states.

15 Many scholars do not include espionage activity in their definition of offensive cyber operations, despite the extensive overlap between cyber capabilities deployed for espionage and disruptive purposes. Even in this narrower definition, some reported operations (e.g., against the Russian Internet Research Agency in 2018, or a North Korea blackout in early 2015 following the Sony Pictures leak) would still count. The U.S. has publicly announced cyber operations against non-state targets such as the so-called Islamic State.

16 David E. Sanger, *Confront and Conceal* (New York: Penguin Random House, 2013); Kim Zetter, *Countdown to Zero Day* (New York: Penguin Random House, 2014); Ronen Bergman and Mark Mazzetti, "The Secret History of the Push to Strike Iran," *New York Times*, September 4, 2019, https://perma.cc/4JL6-4H7L.

But there are good theoretical reasons for being skeptical of a tit-for-tat narrative for cyber operations in general, outside the specific geopolitical context of Iran. First, it centers on the concept of retaliation, thereby assuming that cyber operations are intended to send a message to an adversary, whether about resolve, capability, perception of "red lines" and out-of-bounds targets, or other kinds of signals well explored in IR literature.[17] In other words, a tit-for-tat approach assumes that the purpose of offensive cyber operations is, in Buchanan's terms, signaling not shaping.[18] In contrast, Buchanan argues that cyber capabilities are more suited to shaping, i.e., covert influence. This aligns with a developing consensus in the IR literature that offensive cyber operations are most useful in an "intelligence contest," which is largely (but not entirely) aimed at maneuvering to gain informational, economic, or reputational advantage over an adversary, rather than conventional conflict.[19] This space is often termed the "gray zone," or a situation of "unpeace."[20]

One currently influential approach to cyber operations is known as "persistent engagement."[21] Although persistent engagement is ostensibly a neutral analytical claim about the most appropriate strategy for an "offense-persistent" strategic environment, it has been incorporated centrally into U.S. policy. The current DoD cyber strategy of "defend forward," adopted in 2018, explicitly describes cyber competition in these terms, and is designed to act more flexibly to counter adversaries in their own networks and elsewhere.[22]

17 Joseph S. Nye, "Nuclear Lessons for Cyber Security?," *Strategic Studies Quarterly* 5, no. 4 (2011): 18; Robert Jervis, "Some Thoughts on Deterrence in the Cyber Era," *Journal of Information Warfare* 15, no. 2 (2016): 66–73.

18 Buchanan, *The Hacker and the State*.

19 Max Smeets and Robert Chesney, "Policy Roundtable: Cyber Conflict as an Intelligence Contest," *Texas National Security Review*, September 17, 2020, http://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/.

20 Olga Oliker, "Russian Influence and Unconventional Warfare Operations in the 'Grey Zone:' Lessons from Ukraine," Senate Armed Services Committee Subcommittee on Emerging Threats and Capabilities (2017); Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2017).

21 See e.g., Michael P. Fischerkeller and Richard J. Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," *Orbis* 61, no. 3 (January 1, 2017): 381–93.

22 Max Smeets, "U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection," *Intelligence and National Security* 0, no. 0 (February 15, 2020): 1–10, https://doi.org/10.1080/02684527.2020.1729316.

Persistent engagement approaches agree with the scholars above that cyber operations are most useful in directly shaping a complex and fast-moving environment, but add that by doing so these operations provide ways to implicitly signal to adversaries through "tacit bargaining" and "agreed competition": essentially, showing rather than telling other states what is permissible and what is not. In this way, although persistent engagement accommodates reciprocal signaling at a tactical level, it undermines a tit-for-tat narrative at the strategic level, seeing public incidents are brief glimpses into continuous and tangentially directed cyber campaigns, rather than "loud" signaling for deterrence or other purposes.[23] In particular, Work and Harknett have convincingly applied this lens to Israel-Iran cyber "exchanges" in early 2020, arguing that even if an incident "follows" another—and despite rhetoric like that used by Iranian official in the introduction—we should not necessarily see such events as retaliatory.[24]

Although persistent engagement accommodates reciprocal signaling at a tactical level, it undermines a tit-for-tat narrative at the strategic level, seeing public incidents are brief glimpses into continuous and tangentially directed cyber campaigns, rather than "loud" signaling for deterrence or other purposes.

Although a relatively new insight for cyber operations, this description of the strategic environment resonates with Iranian foreign policy more generally, which involves covert action centrally in two ways.[25] First, its defining feature has been Iran's unacknowledged pursuit of nuclear weapons, which would upset regional geopolitical hierarchies with Israel as the only nuclear-armed state in the region, and—given repeated denials of Israel's right to exist as an independent state by Iranian leaders—threaten Israel and regional stability more generally. Iran's nuclear program and international counter-proliferation efforts have dominated several diplomatic forums and regional relationships for over two decades, culminating

23 Jason Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace," *Journal of Cybersecurity* 5 (January 1, 2019), https://doi.org/10.1093/cybsec/tyz008.

24 J.D. Work and Richard J. Harknett, "Troubled Vision: Understanding Recent Israeli-Iranian Offensive Cyber Exchanges," *Issue Brief* (Washington, D.C: Atlantic Council, July 2020).

25 For an analysis of Iranian (and Israeli) cyber policy in its domestic and regional context, see Gawdat Bahgat, "Iranian-Israeli Confrontation: The Cyber Domain," *Middle East Policy* 27, no. 3 (2020): 115–24, https://doi.org/10.1111/mepo.12516.

in the 2015 Joint Comprehensive Plan of Action (JCPOA) and its divisive consequences for regional allies and U.S. domestic politics.[26]

Importantly, Iran has developed its nuclear program not only through open diplomacy, but also through covert action (for example, using front companies to procure material).[27] These covert actions have led to equally covert responses, such as Israeli leaks of nuclear material, assassinations of key scientists, and sabotage.[28] Cyber operations attributed to both Iran and Israel have been periodically connected to nuclear inspections and negotiations.[29] For the Gulf states, Iranian nuclear threats have led periodically to a doubling down into the U.S. security umbrella, and, more recently, rapprochement for those states that did not already maintain quiet relations with Iran.[30] Covert action is a central aspect of the story of Iran's nuclear program, and so offensive cyber operations are only one part of this broader pattern.

Second, a key feature of Iranian foreign policy and its strategy for regional influence and national security is the use of proxies.[31] This includes conflicts in Syria, where Iranian support for the Al-Assad regime and

---

26 Since the Iranian Revolution in 1979, the United States has put a broad range of sanctions on Iran and its proxies. After a series of reports from the International Atomic Energy Agency stated that Iran was violating the Nuclear Non-Proliferation Treaty, the United States led an international effort to economically isolate Iran. In December 2006, a resolution drafted by Germany passed the UN Security Council. The resolution included an embargo targeting uranium production and enrichment, certain aspects of the Iranian ballistic missile program, and it blocked international transactions that would have assisted the Iranian nuclear or missile programs. These sanctions and restrictions were expanded and strengthened in subsequent Security Council resolutions in 2007, 2008, and 2010. Given how rare security council resolutions are, these were global rebukes of Iranian behavior.

27 See e.g., UN Security Council, "Final Report of the Panel of Experts Established Pursuant to Security Council Resolution 1929 (2010)" (United Nations Security Council, June 11, 2014).

28 Ronen Bergman, *Rise and Kill First: The Secret History of Israel's Targeted Assassinations* (New York: Penguin Random House, 2018); for a more recent interview, see Peter Beaumont, "Ex-Mossad Chief Signals Israel Culpability for Iran Attacks," *Guardian*, June 11, 2021, http://www.theguardian.com/world/2021/jun/11/ex-mossad-chief-yossi-cohen-signals-israel-culpability-for-iran-attacks.

29 Staff Report, "Anti-Israel Group Hacks UN Nuclear Agency Server," *BBC News*, November 28, 2012, https://www.bbc.com/news/world-middle-east-20522585; GReAT, "The Mystery of Duqu 2.0: A Sophisticated Cyberespionage Actor Returns," Securelist—GREAT (Kaspersky Lab), https://perma.cc/EVW3-XS4Q, https://securelist.com/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/70504/.

30 Hussain Ibish, "Saudi Arabia's New Dialogue With Iran Was Long in the Making," *Arab Gulf States Institute in Washington* (blog), May 4, 2021, https://agsiw.org/saudi-arabias-new-dialogue-with-iran-was-long-in-the-making/.

31 This sense of proxies should be distinguished from the "cyber proxy" discussion of front companies masking state tasking, discussed in the following section. It is an open question whether Iranian proxy groups are cyber proxies: relevant incidents include an Israeli kinetic strike on Hamas' "cyber team," Iranian malware in Syria, and similar issues in Yemen. Robert Chesney, "Crossing a Cyber Rubicon? Overreactions to the IDF's Strike on the Hamas Cyber Facility," Lawfare, May 6, 2019, https://perma.cc/5X56-4JMR. Jakub Dalek et al., "Information Controls During Military Operations The Case of Yemen" (Citizen Lab, October 21, 2015); John Scott-Railton et al., "Group5: Syria and the Iranian Connection" (Citizen Lab, August 2, 2016).

Hezbollah is accompanied by open military assistance; and Yemen, where Iran is one player in a shifting web of alliances, and its influence on decision-making is unclear even if its supply of materiel is better understood. Iranian proxy influence also includes unstable states such as Lebanon, Palestine, and Iraq, where sectarian affiliations and complex domestic politics have seen Iranian influence for years, perversely facilitated by the U.S.-led invasion in 2003. Covert action in the gray zone, relying on proxy relationships, is thus a key element of Iranian foreign relations more generally—especially within its self-portrayal as a model of pan-Islamic leadership and anti-colonial resistance.[32]

Convert action in the gray zone . . . is a key element of Iranian foreign operations more generally.

Overall, there are several reasons to look beyond a tit-for-tat narrative around Iranian cyber operations, from initial observations about its application only to Iran rather than other U.S. adversaries, to recent theoretical developments in cyber strategy. These developments suggest that the strategic utility of cyber operations is to achieve continual tactical advantage, signaling only indirectly and tacitly. Such insights chime with broader views of Iranian foreign policy, indicating that "persistent engagement" or similar approaches might well usefully describe Iranian covert action also outside the cyber domain. Despite these critiques, a tit-for-tat narrative persists in policy, professional and media coverage of offensive cyber operations by and against Iran, and the reasons for its staying power are analyzed in the next section.

32 On the workings of Iranian foreign policy, see Luciano Zaccara, "The Iranian Foreign Policy in Turbulent Times: The Arab Uprisings, the Nuclear Deal and the GCC Crisis," *Revista Española de Ciencia Política*, July 24, 2021, 49–70, https://doi.org/10.21308/recp.56.02. More generally, see Ghattas, Kim. *Black Wave: Saudi Arabia, Iran, and the Forty-Year Rivalry That Unraveled Culture, Religion, and Collective Memory in the Middle East*. First. New York: Henry Holt and Company, 2020, 178; Pierre Razoux and Nicholas Elliott, *The Iran-Iraq War* (Cambridge, Massachusetts; London, England: Harvard University Press, 2015).

2. Revisiting Longer-Term Trends in Iranian Cyber Operations

This section revisits longer-term trends in Iranian cyber operations, arguing that the continuation of a tit-for-tat narrative stems from the outsized influence of key early "framing" events, combined with later mirror-imaging of U.S. cyber strategy. Following a brief discussion of data and sources, it is separated into three sections: formative events (2012–2014), a diversified threat (2015 onward), and increased reciprocal tensions (2018 onward). The latter two sections are not exactly chronological, because a diversified threat was not replaced by an increase in tensions—instead, the two continued simultaneously. Crucially, a pattern of unfulfilled expectations emerged with these increased tensions. From 2018 onward, each flashpoint was accompanied by media and industry reporting warning of a substantial tit-for-tat Iranian cyber response, which then subsided without such an attack being publicly reported.

Data and Sources

This section is based on databases of cyber operations worldwide, published and updated by CFR and CSIS.[33] Using these databases, we assembled a list of 80 separate "incidents" of activity either attributed to or targeting Iran between 2012 and 2020, classified according to the categories used by CSIS and CFR (date reported, attribution, target country, target type, type of activity), as well as three additional categories to assess how far such incidents were "responses": reported connection to earlier or later cyber incidents in the list, reported connection to previous non-cyber incidents, and reported non-cyber response if any. We supplemented these databases with several other sources, including landmark studies on Iranian cyber activity published in English and Arabic by research institutes in the U.S. and Middle

33 Although both sources adopt a predominantly discrete, dyadic approach critiqued by the scholarship reviewed in the previous section, they have slight differences. The CSIS database is of "significant cyber incidents," explicitly focusing on specific reports of compromises or other malicious activity, while the CFR database examines cyber operations more broadly, including both "incident" and "threat actor" categorizations. This makes the CFR database—often based on similar or identical sources to the CSIS one—more flexible, meaning that specific threat actors classified according to industry standards, such as the Iran-attributed APT39, do not have to be linked to a particular moment of compromise or adverse effect.

East.[34] In addition to these research reports, we also used U.S. federal indictments, media commentary in major outlets, academic works, and threat intelligence reports by companies mainly in the U.S. and Israel.[35] A summary of the dataset is included in the appendix.

Like all choices around data collection and analysis, this analysis has limitations.[36] These sources are far from neutral: for example, studies suggest that threat intelligence reporting has strong geopolitical affiliations, privileges corporate and government victims over civil society, and we have written elsewhere on its biases in the Iranian context.[37] Equally importantly, threat intelligence companies—like many governments—seek not only to analyze but also to prevent or mitigate Iranian cyber activity. This study therefore omits not only incidents or operations that occur but are not publicly reported (whether due to government classification, company biases, or client confidentiality), but also operations that are detected and mitigated in their early stages before becoming a publicly reported incident.[38] In this way, we focus only on "positive" cases of cyber operations in this section, returning to the distinction between positive and "negative" cases in the following section.[39]

This section is therefore not just a review of Iran-related cyber activity; it is a review of the representation of that activity in the public domain. We identify a tit-for-tat narrative in these representations, rather than ascribing

34 The Carnegie Endowment for International Peace (CEIP, 2018), the International Institute for Iranian Studies in Saudi Arabia (Rasanah, 2020), the King Faisal Centre for Research and Islamic Studies in Saudi Arabia (KFRIS, 2020), the Atlantic Council (Work and Harknett, 2020, cited above), and the Centre for Iranian Studies in Ankara (IRAM, 2021).

35 Checkpoint, Cisco Talos, Clearsky, Crowdstrike, Cylance, Dragos, Fidelis, FireEye, IBM Security, Kaspersky Lab, MacAfee, Recorded Future, and Symantec.

36 Indeed, the plethora of cyber "incident timelines" (which we made ample use of in our research) highlight the tendency to view cyber conflict as a discrete series of engagements. Campaigns are inherently hard to insert into a timeline, which poses a problem for researchers and journalists (often, it's easiest to note the particular date when the U.S. indicted someone for that particular campaign, which can skew our understanding of the timing because the indictment may come months or years after the campaign began.)

37 Lennart Maschmeyer, Ronald J. Deibert, and Jon R. Lindsay, "A Tale of Two Cybers—How Threat Reporting by Cybersecurity Firms Systematically Underrepresents Threats to Civil Society," *Journal of Information Technology & Politics* (June 11, 2020): 1–20; James Shires, *The Politics of Cybersecurity in the Middle East* (London, UK: Hurst, forthcoming).

38 Some such incidents might still be captured by the data here as compromise rather than disruption of the same organizations—so stopped or revealed at an earlier stage. As noted in the previous section, exfiltration is not necessarily separate to disruption.

39 Although for a cautionary note on reporting around sabotage incidents in Iran, see Raz Zimmt, "When It Comes to Iran, Not Everything That Goes Boom in the Night Is Sabotage," *Atlantic Council* (blog), July 30, 2020, https://www.atlanticcouncil.org/blogs/iransource/when-it-comes-to-iran-not-everything-that-goes-boom-in-the-night-is-sabotage/.

the "tit-for-tat" label directly to specific operations or strategies. In other words, this discussion is as much an interrogation of the discourses surrounding Iran-related cyber activity as the activity itself, seeking to limit the methodological problems around opacity mentioned above.

Formative Early Events (2012–2014)

In the summer of 2012, the Shamoon malware deleted data on thousands of computers at Saudi Aramco, also affecting the Qatari company RasGas. A hacktivist group called "The Cutting Sword of Justice" claimed responsibility, but attribution soon settled on Iran. Shamoon occurred shortly after an earlier wiping incident in the Iranian oil sector in April 2012, when the "administrative part" of the oil ministry and connected organizations were severely affected.[40] This wiping malware has not been attributed firmly to any specific actor, although it shared technical characteristics with a malware family also linked to Stuxnet, suggesting that the same actors may have been responsible.[41] The NSA itself has noted how Shamoon demonstrated Iran's "ability to learn" from these incidents: while most analysts read this comment as a technical observation, it can also be understood normatively, as Iran learning the

The NSA itself has noted how Shamoon demonstrated Iran's "ability to learn" from these incidents: while most analysts read this comment as a technical observation, it can also be understood normatively, as Iran learning the appropriate use of cyber capabilities from its adversaries.

40 Kaspersky Lab, "What Was That Wiper Thing?," Securelist—GREAT (Kaspersky Lab), August 29, 2012, https://securelist.com/what-was-that-wiper-thing-48/34088/; Thomas Erdbrink, "Facing Cyberattack, Iranian Officials Disconnect Some Oil Terminals From Internet," *New York Times*, April 23, 2012, https://www.nytimes.com/2012/04/24/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html; Nicole Perlroth, "Cyberattack on Saudi Oil Firm Disquiets U.S.," *New York Times*, October 23, 2012, https://perma.cc/CP22-JCHM; Buchanan, *The Hacker and the State,* pp. 142–145.

41 Flame, a U.S. espionage operation detected in Iran earlier in 2012. There were several 'sons' of Stuxnet; another Israel-attributed virus discovered in 2011, Duqu, was also designed for espionage on industrial control systems. For an overview, see Chronicle, "Who is GOSSIPGIRL? Revisiting the O.G. Threat Actor Supergroup," Medium, April 9, 2019, https://perma.cc/7FVQ-8RTD. For other unattributed wipers discovered around this time in Iran, see Roel Schouwenberg, "GrooveMonitor: Another Wiper Copycat?," Securelist—GREAT (Kaspersky Lab), December 17, 2012, https://securelist.com/groovemonitor-another-wiper-copycat/34811/; Kaspersky Lab, "Narilam: A 'New' Destructive Malware Used In the Middle East," Securelist—GREAT, November 26, 2012, https://securelist.com/narilam-a-new-destructive-malware-used-in-the-middle-east-34/34692/.

appropriate use of cyber capabilities from its adversaries.[42] The *New York Times* noted "suspicions that the Aramco hacking was retaliation" in its initial coverage,[43] and since then Shamoon has been widely presumed to be, if not a direct Iranian response to Stuxnet and related malware, then at least a salvo in the multi-year confrontation over Iran's nuclear program.

Shortly afterward, in late 2012 and 2013, a supposed hacktivist group known as the "Izz ad-Din al-Qassam Cyber Fighters" targeted the U.S. financial sector with distributed denial-of-service (DDoS) attacks. Individuals from two Iranian IT companies—ITSecTeam and Mersad—were later indicted for these DDoS attacks, known as Operation Ababil. In this case, the U.S. government was confident that the operation was a direct response to geopolitical tensions. In the same document quoted above, the NSA assessed that "these attacks are in retaliation to Western activities against Iran's nuclear sector."[44] A closer examination of the regional context reveals that this was not an isolated incident; there had been earlier DDoS attacks against Saudi Arabian targets in 2010 and banks across the Middle East in 2011, viewed also as a reaction to increased sanctions on Iran in this period.[45]

A year or so later, in February 2014, the servers of the Las Vegas Sands casino were hit with malware that ultimately caused $40 million of damage. A few months prior, casino mogul Sheldon Adelson had made a casual suggestion that the U.S. attack Iran with nuclear weapons, and images of Adelson with reference to the nuclear weapons comments appeared on Las Vegas Sands' hacked sites, making the message of retaliation clear. In 2015, Director of National Intelligence James Clapper confirmed on behalf of the U.S. government that the attack came from Iran.[46] While its destructive

42 "Iran—current topics, interaction with GCHQ." Document available from Glenn Greenwald, "NSA Claims Iran Learned from Western Cyberattacks," *Intercept*, February 10, 2015, https://perma.cc/HCQ6-C8YG.

43 Perlroth, "Cyberattack on Saudi Oil Firm Disquiets U.S."

44 "Iran—current topics, interaction with GCHQ." Document available from Greenwald, "NSA Claims Iran Learned from Western Cyberattacks."

45 For a detailed analysis see J.D. Work, "Echoes of Ababil: Re-Examining Formative History of Cyber Conflict and Its Implications for Future Engagements," in *Society of Military History Annual Conference*, 2019.

46 James Clapper, "U.S. Senate Committee on Armed Services: Hearing to Receive Testimony on Worldwide Threats (Transcript)" (Alderson Reporting Company, February 26, 2015).

consequences have been the focus of coverage, other elements, such as exfiltrating private data, have received less attention.[47]

This trio of Iranian cyberattacks ushered in a now-common narrative about cyber "weapons" as a relatively cheap, usable, and deniable tool that enabled countries like Iran to retaliate asymmetrically on the virtual battlefield instead of risking life and limb on the physical one. A cross-domain tit-for-tat narrative is highly appropriate in these cases, understood as asymmetric (although, in the case of Aramco, non-dyadic) responses to provocations either explicitly stated by hacktivist fronts or implicit in the conduct of the operation (an image of a burning U.S. flag for Shamoon, and Adelson's doctored picture for Sands).[48]

This trio of Iranian cyberattacks ushered in a now-common narrative about cyber "weapons" as a relatively cheap, usable, and deniable tool that enabled countries like Iran to retaliate asymmetrically on the virtual battlefield instead of risking life and limb on the physical one.

These three events are formative in U.S. understandings of Iranian cyberactivity and are still frequently cited—almost a decade later—as exemplifying the cyber threat posed by Iran. These three events continue to structure public discussion of the Iranian cyber threat as reactive to both cyber operations (Stuxnet and related wipers), as well as non-cyber events (sanctions and threats). However, broad agreement on their tit-for-tat nature obscures disagreement about more specific aspects, in three ways.

First, the use of hacktivist and corporate proxies for Iranian cyber operations raises similar issues to those around Iranian proxy groups more generally, noted in the previous section: how far is the Iranian state directing their actions, and at what level of control? In his analysis of cyber proxy relationships worldwide, Maurer assesses that these groups were on a "loose leash," suggesting that the time and manner of response is

We should be skeptical of explanatory claims issued by proxy groups.

47 Shires, *The Politics of Cybersecurity in the Middle East,* Chapter 3.

48 Although important critiques of the concept of "asymmetric threat" apply also in the cyber case. See Stephen Blank, "Rethinking the Concept of Asymmetric Threats in U.S. Strategy," *Comparative Strategy* 23, no. 4–5 (October 1, 2004): 343–67, https://doi.org/10.1080/01495930490898759.

determined as much by individual decisions and capabilities (such as building the Brobot DDoS botnet or re-engineering wiping malware), as by specific state instruction.[49] This conclusion suggests we should be skeptical of explanatory claims issued by proxy groups, as they may well be justifying their activity as much to their domestic principals as signaling to the target or other external audiences.[50] This question of state control is central to understanding "responses" in both cyber and kinetic domains.

Second, analysts disagree about the rationality of these three incidents. Influential U.S. policymakers have argued that Iran's tit-for-tat behavior is not only reactive, but irrationally so: Clapper concluded that Iran is a "motivated and unpredictable cyber actor,"[51] while former NSA Director, Keith Alexander, opined that "Iran concerns me the most because they're the ones that will act emotionally while Russia and China are going to be deliberate about what they can do."[52] This frame resonates with broader—discredited—images of Iranian leadership as "mad mullahs" rather than calculative, strategic actors.[53] Others have pointed to a more rational version of the tit-for-tat narrative. Loudermilk concludes that "whenever Iran has conducted cyber operations in response to past conflicts, tensions, or perceived offenses, it has calibrated them to inflict tangible costs and demonstrate strategic reach while maintaining plausible deniability and avoiding escalation."[54] Buchanan's equally sober take is that such calculations are strategic, but mistaken: they are ineffective signaling attempts better suited to "shaping."

This frame resonates with broader—discredited—images of Iranian leadership as "mad mullahs" rather than calculative, strategic actors.

49 Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge New York, NY Port Melbourne New Delhi Singapore: Cambridge University Press, 2018).

50 See, for example, the discussion on the number of computers claimed to be damaged by Shamoon in Shires, *The Politics of Cybersecurity in the Middle East,* Chapter 3.

51 James Clapper, "U.S. Senate Committee on Armed Services: Hearing to Receive Testimony on Worldwide Threats (Transcript)."

52 Joseph Marks, "The Cybersecurity 202: Iran's the Scariest Cyber Adversary, Former NSA Chief Says," *Washington Post*, May 3, 2019.

53 William O. Beeman, *The Great Satan vs. the Mad Mullahs: How the United States and Iran Demonize Each Other* (Chicago: University of Chicago Press, 2008).

54 Micah Loudermilk, "Iran Crisis Moves Into Cyberspace," Washington Institute of Middle East Policy, July 9 2019.

Third, these events did not lead to a "tit-for-tat" response in turn. There is no record of a Saudi response to the Shamoon incident in the public domain, while former CIA Director Michael Hayden suggested that the Sands incident did not deserve U.S. government retaliation (although the perpetrators were later indicted).[55] In contrast, the DDoS campaign did spark more covert industry (and potentially also government) responses, including "hacking back" the Iranian groups themselves.[56] However, these actions are better understood not as reciprocal signals, but as persistent engagement, seeking to counter the DDoS campaign as it happened and interfering with the Brobot network at a tactical level.

A Diversified Threat (2015–)

After the events above, Iranian cyber activity took the form of more dispersed hacking, espionage, and phishing campaigns. From about 2015 onward, Iranian hackers employed phishing attacks against a number of aerospace and satellite companies. In 2018, the United States indicted 10 individuals for a multi-year campaign of "massive, coordinated intrusions" into the servers of hundreds of universities around the world. These individuals, associated with an IRGC-linked entity known as the Mabna Institute, sought to steal intellectual property and data from these universities through phishing and other tactics. These ongoing campaigns, aimed largely at obtaining data rather than at sending a political message, have since become Iran's norm. A wide range of threat intelligence reports details how Iran has hacked U.S. military networks, conducted espionage within the U.S. industrial base, and compromised governments and companies in the Middle East and elsewhere.

Iran has hacked U.S. military networks, conducted espionage within the U.S. industrial base, and compromised governments and companies in the Middle East and elsewhere.

55 "If this would have come across my desk when I was in government, I would have just put it in the outbox." Quoted in Ben Elgin and Michael Riley, "Now at the Sands Casino: An Iranian Hacker in Every Server," *Bloomberg.Com*, December 12, 2014, https://www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas.

56 Nicholas Schmidle, "The Digital Vigilantes Who Hack Back," *New Yorker*, April 30, 2018, https://perma.cc/X7S8-DQSJ.

This "turn" to espionage must be placed in the longer context of Iranian cyber-espionage conducted against dissidents and political opposition, rather than commercial or international security targets. Although first institutionally based in the Ministry of Intelligence and Security (MOIS), rather than the IRGC-affiliated actors above, Iranian cyber-espionage has a long history. As Anderson and Sadjadpour note, Iran's response to the popular Green movement in 2009 included pro-regime website defacement and disruption, while the landmark compromise of Dutch certificate authority Diginotar in 2011 was intended to facilitate domestic surveillance.[57] This parallel strand of cyber-espionage has continued and expanded worldwide in recent years: as Michaelson demonstrates in his study of what he calls "transnational repression," Iran regularly deploys techniques such as social engineering, phishing, and disinformation against political opposition outside its borders.[58] Such espionage activity then, is not a turn away from disruptive responses but an institutional expansion of cyber-espionage from repression toward wider national security purposes.

Espionage activity is not a turn away from disruptive responses but an institutional expansion of cyber-espionage . . .

Iran's disruptive activity continued in this period with the deployment of wipers in its immediate neighborhood. Most notably, "Shamoon 2.0" affected the networks of multiple organizations in the Saudi government between November 2016 and February 2017. Shamoon 2 was, in some ways, a clear signal communicated through associated political images: rather than a burning U.S. flag, this wiper used a picture of Alan Kurdi, a Syrian child photographed drowned on a Greek beach in September 2015. Signals were also embedded in the fabric of the malware itself: it set the date on infected computers to August 2012 (shortly before the original Shamoon had begun to wipe data on Aramco networks) and instructed the computer to wipe itself when the computer clock reached the time Shamoon had occurred. Despite these signals, Shamoon 2 was not clearly responsive, with no easily identifiable provocation other than generally increased tensions between Iran and

57 Collin Anderson and Karim Sadjadpour, "Iran's Cyber Threat: Espionage, Sabotage, and Revenge" (Carnegie Endowment for International Peace, 2018).

58 Marcus Michaelsen, "Silencing Across Borders: Transnational Repression and Digital Threats against Exiled Dissidents from Egypt, Syria and Iran" (The Hague: Hivos, 2020), https://researchportal.vub.be/en/publications/silencing-across-borders-transnational-repression-and-digital-thr.

Saudi Arabia. These tensions included low-level website defacements on both sides, termed the start of a "cyberwar" by international media.[59]

The Shamoon 2 wiper was also integrated into malware designed for espionage and ransomware, designed with the option to restore encrypted data after payment, rather than delete data irreversibly.[60] These alterations represent a wider shift in Iranian cyber activity toward ransomware, with a notable ransomware strain infecting multiple U.S. organizations at a similar time.[61] Security researchers have continued to observe Iranian ransomware development since then, with compromises of Israeli companies in 2020.[62] Documents leaked in early 2021 suggest this focus is a deliberate strategic decision for IRGC-affiliated companies.[63] Most recently, a threat actor named "Agrius," first reported in May 2021 and tentatively linked with Iran, has deployed ransomware against Israeli organizations, developed from earlier wiping modules that contained messages about critical infrastructure in the UAE.[64] As well as demonstrating the continued integration of political signaling into wiper modules, these reports echo an ambiguity between destruction and extortion which has surfaced in state-sponsored operations by Russia and North Korea.[65] In the Iranian case, it is the legacy of earlier formative incidents that pushes analysts toward assessments of a more destructive intent.[66]

These reports echo an ambiguity between destruction and extortion . . .

59 Shahin Azimi, "Iran-Saudi Tensions Erupt in 'Cyberwar,'" *BBC News*, June 3, 2016, https://perma.cc/8PH3-Z6LY.

60 E.g. Kaspersky Lab, "From Shamoon to Stonedrill: Wipers Attacking Saudi Organizations and Beyond" (Kaspersky Lab Global Research and Analysis Team, March 7, 2017). These connections suggest that an IRGC-linked group known as APT33 was likely responsible. For further discussion, see Shires, *The Politics of Cybersecurity in the Middle East,* Chapter 3.

61 Department of Justice, "Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses," Office of Public Affairs, November 28, 2018, https://perma.cc/JA9E-P34N.

62 ClearSky Cybersecurity, "Pay2Kitten—Fox Kitten 2," December 17, 2020, https://www.clearskysec.com/pay2kitten/.

63 Flashpoint, "Second Iranian State-Sponsored Ransomware 'Project Signal' Emerges," *Flashpoint Intel* (blog), April 30, 2021, https://www.flashpoint-intel.com/blog/second-iranian-ransomware-operation-project-signal-emerges/; Clearsky Research Team, "Operation Quicksand," *Clearsky Cyber Security* (blog), October 15, 2020, https://www.clearskysec.com/operation-quicksand/.

64 Amital Ben Shushan Ehrlich, "From Wiper to Ransomware: The Evolution of Agrius" (Sentinel Labs Research Team, May 2021).

65 Buchanan, *The Hacker and the State*, Chapter 12. For an in-depth analysis of one incident, see Joe Slowik, "Spyware Stealer Locker Wiper: Lockergoga Revisited" (Dragos Inc., March 2020), https://www.dragos.com/blog/industry-news/spyware-stealer-locker-wiper-lockergoga-revisited/.

66 For an expansion of this argument, see Shires, *The Politics of Cybersecurity in the Middle East,* Chapter 3.

Overall, this diversified threat, including espionage for repressive and strategic purposes, ransomware, and wipers, starkly contrasts with the responsive character of the formative events above. While wiping operations continued to target Iranian adversaries in the region, especially organizations linked to Saudi Aramco, with varying levels of political signaling, they were not explicitly responsive and so do not support a tit-for-tat narrative. Furthermore, there was no publicly reported cyber response to Shamoon 2 from Saudi Arabia or Iran's other adversaries, although Iran's cyber contractor and hacking scene was subject to significant internal tension and pressure during this period. Most starkly, a former key participant in Iranian cyber operations was reportedly assassinated by Iranian government operatives in 2016.[67] Whether these internal tensions and divisions were due to adversary covert operations is impossible to tell from the public record, but it would not be out of keeping with similar actions against Iranian targets in other spheres.[68]

Unfulfilled Expectations (2018–)

The tit-for-tat narrative became more prominent after more aggressive action against Iran by the U.S. government from 2018 onward, especially the Trump administration's withdrawal from the JCPOA in summer 2018. This more aggressive posture included cyber operations, both explicitly acknowledged by Cyber Command as discussed below, and others reportedly authorized by a Presidential finding in 2018 enabling the CIA to conduct more offensive cyber operations, including several against Iran.[69]

Before the JCPOA withdrawal, analysts expected to see Iran hit back using its cyber toolkit.[70] CSIS' James Lewis told the *New York Times*, "Until

67 Levi Gundert, Sanil Chohan, and Greg Lesnewich, "Iran's Hacker Hierarchy Exposed" (Recorded Future Insikt Group, May 9, 2018). See also note 84 below.

68 Bergman, *Rise and Kill First*.

69 Zack Dorfman et al., "Exclusive: Secret Trump Order Gives CIA More Powers to Launch Cyberattacks," Yahoo News, July 15, 2020, https://news.yahoo.com/secret-trump-order-gives-cia-more-powers-to-launch-cyberattacks-090015219.html.

70 See e.g., Mike Chapple, "Ditching Iran Nuclear Deal Will Leave U.S. Open to Dangerous Cyberattacks," CNBC Commentary, May 10, 2018, https://www.cnbc.com/2018/05/10/ditching-iran-nuclear-deal-will-leave-us-open-to-dangerous-cyberattacks.html; Andy Greenberg, "The Iran Nuclear Deal Unraveling Raises Fears of Cyberattacks," *Wired*, May 9, 2019, https://www.wired.com/story/iran-nuclear-deal-cyberattacks/.

today, Iran was constrained . . . With the deal's collapse, they will inevitably ask, 'What do we have to lose?'"[71] Within a day of the announcement, CrowdStrike and others reported that Iranian hackers were targeting Western diplomats. Yet this seemingly quick-hit response was not followed by a major Shamoon-like attack. A few months after the pullout, reports surfaced of Iranian campaigns against industrial control systems around the world, Iranian involvement in Facebook-based disinformation efforts, and Iranian hackers targeting university websites for intellectual property theft. All three were quieter, campaign-style efforts with no clear connection to the withdrawal.

The incident that most closely fits expectations of a response to the JCPOA withdrawal was "Shamoon 3," which occurred in December 2018, deleting data on hundreds of computers in the business networks of Italian energy company Saipem, whose biggest client is Saudi Aramco.[72] However, it is unclear whether this incident was a response at all and, if so, to what. The malware included an image of a multivalent Quranic verse condemning "Abu Lahab" (the father of flame).[73] Whatever the intended signal, there were other reported events in the intervening period that were equally plausible triggers: for example, an "updated" Stuxnet was reportedly deployed on Iranian networks in October 2018.[74]

71 Nicole Perlroth, "Without Nuclear Deal, U.S. Expects Resurgence in Iranian Cyberattacks," *New York Times*, May 11, 2018, https://www.nytimes.com/2018/05/11/technology/iranian-hackers-united-states.html.

72 The impact of this incident was unclear: Reuters reported that Saipem's computers were "crippled," but their source noted that Saipem had promptly installed back-ups, so no data was lost. Stephen Jewkes and Jim Finkle, "Saipem Says Shamoon Variant Crippled Hundreds of Computers," Reuters, December 13, 2018, https://www.reuters.com/article/us-cyber-shamoon-idUSKBN1OB2FA.

73 In their analysis linking this incident to Iranian IRGC-linked group APT33, the McAfee analysts do not speculate on the meaning of this image. In the Quran, Abu Lahab was Muhammad's uncle, notorious for his disbelief in the prophet's revelations and a marriage dispute over Muhammad's daughters. The ubiquity of this figure means it is difficult to infer any link to previous U.S. or other actions (although, of course, "Flame" was the name of an earlier malware discovered in Iran). Thomas Roccia, Jessica Saavedra-Morales, and Christiaan Beek, "Shamoon Attackers Employ New Tool Kit to Wipe Infected Systems," *McAfee Blogs* (blog), December 19, 2018, https://www.mcafee.com/blogs/other-blogs/mcafee-labs/shamoon-attackers-employ-new-tool-kit-to-wipe-infected-systems/.

74 Staff Report, "TV Report: Israel Silent as Iran Hit by Computer Virus More Violent than Stuxnet," *Times of Israel*, October 31, 2018, https://perma.cc/2PQG-U6TJ.

In contrast, from 2019 onward, several U.S. cyber operations against Iran were explicitly responsive, couched in terms of "proportionate" retaliation to avoid escalation.[75] In June 2019, the U.S. accused Iran of attacks on oil tankers in the Gulf of Oman, and about a week later the IRGC shot down a U.S. drone. The United States soon responded with an offensive cyber operation, having reportedly aborted plans for a retaliatory military strike. According to media reports, the U.S. Cyber Command conducted a disruptive operation against a group that had been tracking shipping for the IRGC, disabling their systems.[76] A second cyber operation occurred in response to drone attacks on Saudi Arabian oil facilities in September 2019, which Secretary of State Mike Pompeo called an "act of war."[77] In this case, the U.S. targeted Iran's ability to distribute propaganda.[78] A year later, the U.S. again conducted cyber operations seeking to deter and disrupt Iranian disinformation campaigns around the 2020 Presidential elections.[79] In tandem with these cyber operations, the U.S. also responded to Iranian activity with an increase in legal measures, unsealing federal indictments and Treasury sanctions against 85 individuals, and several corporate entities, for cyber activities connected to both the IRGC and MOIS over the last five years. Other unattributed incidents suggest more covert forms of retaliation from unknown actors: for example, after the Abqaiq incident, a reported cyberattack in September 2019 supposedly targeted Iranian oil installations.[80]

From 2019 onward, several U.S. operations against Iran were explicitly responsive, couched in terms of "proportionate" retaliation . . .

75 Brandon Valeriano and Benjamin Jensen, "How Cyber Operations Can Help Manage Crisis Escalation with Iran," *Washington Post*, June 25, 2019, https://perma.cc/8C8R-ASJL.

76 Wagtendonk, Anya van. 2019. "Trump Called off a Military Strike against Iran. The U.S. Targeted Its Computer Systems Instead." *Vox*, June 23, 2019. https://perma.cc/UW9A-23BS.

77 Nicole Gaouette et al., "Pompeo Says Saudi Attack an 'act of War' as Trump Sounds More Cautious Note," *CNN*, September 19, 2019, https://perma.cc/2LZ3-QR3L.

78 Idrees Ali and Phil Stewart, "Exclusive: U.S. Carried out Secret Cyber Strike on Iran in Wake of Saudi Oil Attack: Officials," Reuters, October 16, 2019, https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive-idUSKBN1WV0EK.

79 Jamie Tarabay and Kartikay Mehrota, "Iran Targeted by U.S. Over Threats Against Democratic Voters," *Bloomberg.Com*, October 22, 2020, https://www.bloomberg.com/news/articles/2020-10-22/iran-takes-center-stage-as-u-s-cites-election-hacking-concerns; Ellen Nakashima, "U.S. Undertook Cyber Operation against Iran as Part of Effort to Secure the 2020 Election," *Washington Post*, November 4, 2020.

80 Staff Report, "Iran Denies Successful Cyber Attacks On Oil Sector," RadioFarda (Agence France Presse), September 21, 2019, https://perma.cc/ZP7Z-VLA2.

High expectations of an Iranian cyber response to these U.S. cyber operations went unfulfilled. Cyber firms like FireEye warned that the rise in tensions coincided with an uptick in Iranian efforts to compromise U.S. networks,[81] although a later report notes that heightened cyber activity *preceded* the downing of the U.S. drone.[82] Importantly, this relative lack of response was unlikely to be due to insufficient capability. Leaked documents purportedly from Iranian IRGC-linked groups, surfacing in May 2019 potentially due to a U.S. hack-and-leak operation, indicated that they had been tasked to develop disruptive capabilities for industrial control systems.[83] This assessment was supported by reports of Iranian intrusions into Bahraini critical infrastructure in June 2019, as well as hype from earlier probes of a U.S. dam, and the mistaken Iranian attribution of the "Triton" malware in a Saudi petrochemical facility in 2017.[84] When the expected response to U.S. cyber operations did not occur, some cybersecurity analysts claimed instead that "Iran may be waiting to launch destructive attacks" until a more appropriate moment.[85]

---

81 Andy Greenberg, "Iranian Hackers Launch a New U.S. Campaign as Tensions Mount," *Wired*, June 20, 2019, https://perma.cc/H5YC-75HT.

82 Annie Fixler, "The Cyber Threat from Iran after the Death of Soleimani," *CTC Sentinel* 13, no. 2 (February 27, 2020), https://ctc.usma.edu/cyber-threat-iran-death-soleimani/.

83 Gordon Corera, "Russian Hackers Cloak Attacks Using Iranian Group," *BBC News*, October 21, 2019, https://perma.cc/G3BX-2AC5; Catalin Cimpanu, "New Leaks of Iranian Cyber-Espionage Operations Hit Telegram and the Dark Web," ZDNet, May 9, 2019, https://perma.cc/MRN6-QUFC. Some leaks associate the development of ICS malware with specific organizations associated with the IRGC: the "Rana Institute" and the "Kavesh center for IT security incidents." Clearsky Cybersecurity, "Iran Nation-State APT Groups 'Black Box' Leak," May 2019. Although the leaked Kavesh project was unsuccessful (according to the leaks themselves, via Clearsky), more recent leaks suggest a wider range of ICS targeting allegedly by IRGC-affiliated organization "Shahid Kaveh," and so despite the failure of individual projects, overall capability is likely to be sufficient: Deborah Haynes, "Iran's Secret Cyber Files on How Cargo Ships and Petrol Stations Could Be Attacked," Sky News, July 28, 2021, https://news.sky.com/story/irans-secret-cyber-files-on-how-cargo-ships-and-petrol-stations-could-be-attacked-12364871. On the possibility that the 2019 leaks were the result of a CIA operation, see Zack Dorfman et al., "Secret Trump Order Gives CIA More Powers to Launch Cyberattacks."

84 U.S. Department of Justice, "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector" (Office of Public Affairs, March 24, 2016), https://perma.cc/S7YF-DZGP. A key participant in Iranian cyber operations, associated with both the intelligence ministry and the IRGC, claimed—via an Iranian opposition journalist—that the "Khaybar Center for Information Technology" was responsible for the dam operation, as well as other incidents including a 12-hour power cut in Turkey. As noted above, this individual was reportedly assassinated by Iranian government operatives in 2016, and his journalist contact, Ruhollah Zam, was sentenced to death and hanged in December 2020. For more details, see Gundert et al., "Iran's Hacker Hierarchy Exposed" and Saleh Hamid, "Secret details emerge on Iran's Cyber Army," *Al-Arabiya*, January 15, 2017, https://perma.cc/Q6XA-PCUX. On TRITON attribution, see FireEye, "Attackers Deploy New ICS Attack Framework 'TRITON' and Cause Operational Disruption to Critical Infrastructure," FireEye, December 14, 2017, https://perma.cc/HVK5-2WGB. Pierluigi Paganini, "Triton Malware Was Developed by Iran and Used to Target Saudi Arabia," *Security Affairs*, December 16, 2017, https://perma.cc/JTC7-ABJM.

85 Recorded Future analyst Levi Gundert in Robert Scammell, "Iranian Threat Actor APT33 Steps up Cyberattacks on Saudi Arabia," *Verdict*, June 27, 2019, https://perma.cc/J7FD-MJTU.

The years 2020 and 2021 saw further expectations of major Iranian cyber-attacks. As explored in detail by Work and Harknett, Israeli and Iranian cyber operations in early 2020 were interpreted by many observers as tit-for-tat signaling, although their analysis suggests a persistent engagement approach provides greater understanding. Again, in July 2020, U.S. media predicted a "renewal of cyberattacks" by Iran following these tensions which did not materialize.[86] Meanwhile, unattributed reports of cyber incidents percolated through Iranian media, including a widespread DDoS operation against Iranian government systems in February 2020.[87] Reciprocal accusations of maritime sabotage in early 2021, and reported Israeli action against Iran's nuclear program shortly afterward, led to further unfulfilled expectations of Iranian cyber responses, epitomized by the quotation with which we opened this paper.[88]

The years following U.S. withdrawal from the JCPOA cemented a pattern of unfulfilled expectations.

Overall, the years following U.S. withdrawal from the JCPOA cemented a pattern of unfulfilled expectations: each point of tension was accompanied by media and industry reporting warning of an Iranian cyber response along the lines of Shamoon, Sands, or even sabotage of industrial control systems. Each point of tension subsided without such an attack occurring. There are several potential reasons for this pattern, including the efforts of cybersecurity companies and governments to thwart specific operations, a broader degradation of Iranian capability, or even the success of U.S. and allies' signaling that any such operation would be met with serious consequences, thereby dissuading the Iranian leadership from sanctioning such operations by their proxies. While each of these explanations is an important part of the whole picture, they are together insufficient. Iranian cyber capabilities appear to have increased rather than degraded overall, the sheer range of potential targets and their lack of sufficient defenses makes it unlikely that

86 Sanger, Schmitt, and Bergman, "Long-Planned and Bigger Than Thought."

87 Davey Winder, "Powerful Cyber Attack Takes Down 25% Of Iranian Internet," *Forbes*, February 9, 2020, https://www.forbes.com/sites/daveywinder/2020/02/09/powerful-iran-cyber-attack-takes-down-25-of-national-internet/.

88 We note that the targets of previous U.S. and Israeli operations against "shipping databases" appear to be as much preventative as signaling, looking to hinder Iranian ability to carry out such maritime sabotage. These operations are also likely based on cyber intelligence gathering operations also designed to prevent such sabotage. More generally, U.S. and Israeli cyber-espionage continues against Iran, suggesting this is a classic intelligence contest: seeking information of value, while also countering others' campaigns.

defenders would prevail all the time, and the riskier kinetic operations attributed to Iran suggest that dissuasion is an unlikely factor.

Instead, we suggest an alternative explanation: that expectations of Iranian cyber responses are a combination of two interpretive errors. The first is the excessive power of early formative events in shaping assessments of Iranian intent. Several studies suggest that "framing" effects are highly significant in the overall understanding of cyber threats,[89] and so the outdated perception that Iranian cyber actors are responsive, unpredictable, and even irrational could be the driver behind such expectations. We recognize that a reliance on these formative events in public discussions of Iranian cyber activity may well be deliberate, in order to emphasize risks to skeptical audiences, or to stand in for more current threat intelligence that cannot be disclosed. If this is the case, then the encouragement of inaccurate expectations is a downside to this deliberate strategy that should be taken seriously, as it distorts the broader discourse around Iranian cyber activity.

The other interpretive error is mirror-imaging U.S. strategy; a mistake that has been shown to have serious consequences in other conflict zones and previous eras of tension.[90] In this case, the shift in U.S. posture from legal measures and defensive actions toward more offensive operations, explicitly designed and communicated as reactive, may well lead analysts to expect Iranian decision-makers to think in the same way. This longer-term review of Iranian cyber operations suggests that Iran does not mirror the U.S. perspective: the strategic benefit from worldwide espionage and disinformation, along with sporadic regional disruption not connected to any particular provocation, seems to far outweigh the advantage gained from a briefly impactful but difficult-to-control and potentially reputationally

The shift in U.S. posture from legal measures and defensive actions toward more offensive operations, explicitly designed and communicated as reactive, may well lead analysts to expect Iranian decision-makers to think in the same way.

89 Dunn Cavelty, "Cyber-Terror—Looming Threat or Phantom Menace?"; Dunn Cavelty, "From Cyber-Bombs to Political Fallout"; Lawson, "Beyond Cyber-Doom."

90 Nicholas Ross Smith, "The Re-Emergence of a 'Mirror Image' in West–Russia Relations?" *International Politics* 55, no. 5 (September 1, 2018): 575–94, https://doi.org/10.1057/s41311-017-0095-z.

damaging cyber operation.[91] In order to explore this argument in detail, the next section turns to one specific case of unfulfilled expectations of a cyber response: the killing of Qassem Suleimani in January 2020.

91 In this lens, a more recent focus on ransomware fits well with the priorities of an extensively sanctioned and economically deprived regime, and so should not be discounted merely as a cover for wiping activity.

3. Cyber Operations after the Qassem Suleimani Killing

This section suggests we can learn more about Iran's cyber strategy by looking not only at where incidents do occur (the positive cases that formed the majority of the discussion in the previous section), but also by looking in more detail at "negative cases" where we expect incidents to occur, but they do not.[92] In this section, we argue that a lack of cyber response to the killing of Qassem Suleimani indicates that Iran's cyber strategy is far more regionally attuned and domestically influenced than generally assumed.

The Killing of Qassem Suleimani

The United States killed Qassem Suleimani on January 3, 2020, in a drone strike at Iraq's Baghdad Airport, along with Abu Mahdi Al-Muhandis, deputy leader of an influential Iraqi Shia militia, and several others. Suleimani was the commander of the IRGC special operations division called the Quds Force. During his tenure as commander, Suleimani was integral to building Iran's "Axis of Resistance" in Iraq, Syria, Lebanon, and Yemen by developing relationships with groups widely considered to be Iranian proxies through training, funding, supply, and coordination. Suleimani was a low-profile, highly respected commander who enabled Iran to wield an outsized regional influence given its economic issues.

Suleimani's death was the culmination of increasing tensions between the U.S. and Iran throughout 2019, discussed in the previous section. Outside the narrow lens of cyber operations, this escalation displayed a clear retaliatory dynamic in the lead-up to the U.S. strike in Baghdad.[93] In April 2019,

92 Negative cases are generally overlooked in scholarship on cyber strategy, as it is very difficult to draw firm conclusions from something that did not happen (and, of course, they do not appear in the databases used in the previous section). However, negative cases are useful for highlighting interpretive errors in discourses.

93 It should be noted that the interpretation of kinetic responses is also vulnerable to mirror imaging errors. For a description of recent militia attacks and U.S. communication around airstrikes in response (explicitly described as "tit-for-tat" by analysts) see John Kirby, "Statement by the Department of Defense" (U.S. Department of Defense, June 27, 2021), https://www.defense.gov/Newsroom/Releases/Release/Article/2672875/statement-by-the-department-of-defense/; Phil Stewart and Idrees Ali, "Undeclared Conflict? America's Battles with Iran-Backed Militia Escalate, Again," Reuters, June 29, 2021,

the Trump administration designated the IRGC a foreign terrorist organization. In late 2019, Iranian-backed militias in Iraq conducted a series of attacks against bases housing U.S. personnel. On December 27, 2019, one of those attacks killed an American military contractor. In response to these attacks, the U.S. launched airstrikes in Iraq and Syria against militias supported by Iran. In turn, militia supporters in Iraq then attempted to storm the U.S. embassy in Baghdad.

While the U.S. justified its killing of Suleimani as "deterring future Iranian attack plans," this rationale was muddied by tweets from President Trump stating that Iran would pay a "very big price" shortly before the strike.[94] A subsequent report by the UN Special Rapporteur on Extrajudicial Killings concluded that the U.S. strike was unlawful under international law due to the lack of an "imminent" threat, although this conclusion was rejected by the U.S.[95] Assessing the presence or absence of sufficient threat intelligence justifying the strike is beyond the scope of this study: it is sufficient to note that this strike fits within the broader escalatory and retaliatory pattern between the U.S. and Iran sketched in the previous paragraph.

Iran then launched missile attacks on bases hosting U.S. personnel on January 7, 2020.[96] These missile attacks were justified by Iranian foreign minister Javad Zarif as a "proportionate" response to the U.S. drone strike, who tweeted (in English, to an international audience): "Iran took & concluded proportionate measures in self-defense under Article 51 of UN Charter targeting base from which cowardly armed attack against our

https://www.reuters.com/world/middle-east/undeclared-conflict-americas-battles-with-iran-backed-militia-escalate -again-2021-06-29/.

94 "U.S. Drone Strike in Iraq Kills Iranian Military Leader Qasem Soleimani." *American Journal of International Law* 114, no. 2 (n.d.): 313–23. See also Trump's other comments, such as "They attacked us, & we hit back. If they attack again, which I would strongly advise them not to do, we will hit them harder than they have ever been hit before!" Fred Pleitgen, Tim Lister, and Schams Elwazer, "Exclusive: Iran's Response to U.S. Will Be Military—Khamenei's Adviser," *CNN*, January 5, 2020, https://www.cnn.com/2020/01/05/middleeast/iran-soleimani-khamenei-adviser-intl/index.html.

95 UN Human Rights Council, "Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions" (United Nations, June 29, 2020), pp. 35–38.

96 U.S. Department of Defense. "DOD Statement on Iranian Ballistic Missile Attacks in Iraq." Accessed April 8, 2021. https://www.defense.gov/Newsroom/Releases/Release/Article/2052103/dod-statement-on-iranian-ballistic-missile-attacks-in-iraq/.

citizens & senior officials were launched. We do not seek escalation or war, but will defend ourselves against any aggression."[97]

Expectations of a Cyber Component

Before the missile attacks on the Ayn al-Asad and Erbil airbases, many commentators suggested that an Iranian response would involve cyber operations. This expectation was helped by Iranian statements in the immediate aftermath emphasizing the range of capabilities available to mount a response, and the legitimacy of responding with "any means." However, given the proxy-based command structure of many Iranian cyber operations, as well as their many commercial and critical infrastructure targets, claims by senior Iranian officials that a response would be "military . . . against military sites" suggested that cyber operations may not be strategically appropriate.[98]

On January 6, 2020, the United States Cybersecurity and Infrastructure Agency (CISA) warned of a "potential Iranian cyber response" to the U.S. strike, citing Iran's "historic use of cyber offensive activities to retaliate against perceived harm," and giving as examples Operation Ababil, the Bowman dam intrusion, and the Sands casino wiper.[99] An FBI advisory contained similar warnings of "computer network operations against U.S.-based networks in retaliation for last week's strikes," citing an increased detection of Iranian reconnaissance activity.[100] U.S. experts interviewed by the *Washington Post* for an article on January 3 communicated an even clearer message, claiming that "a cyberattack should be expected," and "the focus will be on critical infrastructure—oil

97 Javad Zarif. "Iran Took & Concluded Proportionate Measures in Self-Defense under Article 51 of UN Charter Targeting Base from Which Cowardly Armed Attack against Our Citizens & Senior Officials Were Launched. We Do Not Seek Escalation or War, but Will Defend Ourselves against Any Aggression." Tweet. *@JZarif* (blog), January 8, 2020. https://twitter.com/JZarif/status/1214736614217469953. For the perceived proportionality of this response, see also Pleitgen, Lister, and Elwazer, "Exclusive: Iran's Response to U.S. Will Be Military—Khamenei's Adviser," where the Iranian official states that "The only thing that can end this period of war is for the Americans to receive a blow that is equal to the blow they have inflicted. Afterward they should not seek a new cycle."

98 Pleitgen, Lister, and Elwazer, "Exclusive: Iran's Response to U.S. Will Be Military—Khamenei's Adviser."

99 Cybersecurity and Infrastructure Agency. "Potential for Iranian Cyber Response to U.S. Military Strike in Baghdad | CISA." Accessed April 11, 2021. https://us-cert.cisa.gov/ncas/alerts/aa20-006a.

100 Sean Lyngaas, "FBI Says Iranian Hackers Have Stepped up Reconnaissance since Soleimani Killing," *CyberScoop*, January 10, 2020, https://www.cyberscoop.com/fbi-iran-soleimani-cyber/.

and gas in the Middle East, maybe elsewhere."[101] Like the CISA alert, the *Washington Post* article drew on all three formative early events detailed in the previous section to make the case for a likely substantial cyber response, albeit caveating that it was "difficult to predict what an Iranian offensive in cyberspace would look like."[102]

Industry assessments were equally expectant, with a detailed blog by Recorded Future published on the day of the missile attacks running through a wide range of Iranian threat actor groups, as well as Shamoon and other Iranian wipers and ransomware.[103] Even after the missile attacks, many believed that those attacks did not constitute the entirety of a response to the killing of one of Iran's most senior and influential generals. On January 10, FireEye announced increased efforts to detect Iranian activity following the reconnaissance noted above, reasoning that an Iranian cyber response "could include cyber espionage intrusions as well as disruptive or destructive cyber attacks."[104] ICS security firm Radiflow went further, publishing a paper titled "In the Aftermath of the Assassination: Fear of Cyber-Retaliation by Iranian Attack Groups" on January 15 that predicted a range of cyber responses, including in ICS networks.[105]

These expectations across U.S. government, media, and the threat intelligence industry went largely unfulfilled. Before discussing cyber operations that did take place around the time of the Suleimani killing but were discounted as a response, it is useful to note how both interpretive errors identified in the previous section appear here. First, the early formative

101 Romm, Tony, Isaac Stanley-Becker, and Craig Timberg. "'A Cyberattack Should Be Expected': U.S. Strike on Iranian Leader Sparks Fears of Major Digital Disruption." *Washington Post*. Accessed April 11, 2021. https://www.washingtonpost.com/technology/2020/01/03/cyber-attack-should-be-expected-us-strike-iranian-leader-sparks-fears-major-digital-disruption/.

102 Ibid.

103 Insikt Group, "Iranian Cyber Response to Death of IRGC Head Would Likely Use Reported TTPs and Previous Access," *Recorded Future* (blog), January 7, 2020, https://www.recordedfuture.com/iranian-cyber-response/.

104 John Hultquist, "FireEye Response to Mounting U.S.-Iran Tensions: Preparing for Possible Iranian Cyber Attacks," FireEye, January 10, 2020, https://www.fireeye.com/blog/products-and-services/2020/01/fireeye-response-to-mounting-us-iran-tensions.html.

105 Radiflow Cyber Research Team, "In the Aftermath of the Assassination: Fear of Cyber-Retaliation by Iranian Attack Groups," Security Brief (Radiflow, January 15, 2020). Although the report is dated 2019, monitoring services suggest it was published on January 15: https://statoperator.com/research/cyber-daily-news-2020-01-15/ For an excellent overview of ICS risks in the region, see Selena Larson and Sergio Caltagirone, "Industrial Cyberattacks in the Middle East and International Consequences," in *Cyber War & Cyber Peace in the Middle East: Digital Conflict in the Cradle of Civilization*, ed. Michael Sexton and Eliza Campbell (Middle East Institute, 2020), 37–55.

events—Shamoon, Op Ababil, and the Sands casino wiper—remained the main justification for expecting an Iranian cyber operation targeting U.S. organizations or networks. As noted above, it is possible that these events were deliberately substituted for more recent events that cannot be disclosed, but the effect is the same: an increasingly distant inference from actions taken many years earlier, despite extensive changes to the strategic landscape and Iranian cyber capabilities in the intervening period.

Second, these expectations also display an implicit mirror-imaging of the U.S. understanding of cyber capabilities as a de-escalatory, proportionate response, drawing on the U.S. cyber operations against Iran in 2019. The commentary above emphasizes how Iran would seek to avoid further escalation in an already highly inflammatory situation: however, it was the *American* perspective that viewed offensive cyber operations as the most appropriate retaliatory tool in such a situation. There is no indication, even from leaked strategic documents from IRGC-linked cyber teams, that this perspective is also is part of the Iranian calculus. Instead, as suggested by the previous section, Iranian strategic understandings of the utility of cyber operations focus on a persistent operational effort to obtain intelligence, spread supportive narratives, and suppress political opposition, punctuated by more disruptive events that are precisely not clearly tied to specific prior events.

Iranian strategic understandings of the utility of cyber operations focus on a persistent operational effort to obtain intelligence, spread supportive narratives, and suppress political opposition, punctuated by more disruptive events that are precisely not clearly tied to specific prior events.

Cyber Operations around the Suleimani Killing

To explore these interpretive errors in more detail, we can turn from what U.S. commentators got wrong about a cyber response—which is, admittedly, far easier to observe with hindsight—to what they got right. There were two cyber events occurring around this time, in addition to the increased reconnaissance and disinformation activity observed by the

analysts above, that were not understood as an Iranian response despite potential for doing so.[106]

The first event was a set of website defacements explicitly claiming to respond to the U.S. strike on Suleimani, later detailed in a U.S. federal indictment.[107] The indictment states that Behzad Mohammedzadeh, a 19-year-old Iranian, based in Iran, received access information to at least seven websites from a Palestinian associate and uploaded Suleimani-themed content to these websites on January 7, the same day as the official Iranian response. The websites then displayed pictures of Suleimani and the message "down with America" rather than their usual content. These defacements sit in a long line of "hacktivist" actions by young Iranians, some of whom later went on to work with reported state-affiliated companies.[108] While these defacements were mentioned in the commentary above, the history of Iranian hacktivism and lack of state connection meant that these defacements were correctly downplayed, and not seen as part of an Iranian response to the killing despite their explicit signaling.

The second event was a wiper variant named "Dustman" identified by the Saudi National Cybersecurity Authority (NCA) in December 2019.[109] Dustman was publicly attributed to Iranian-linked groups by reporters for *CyberScoop* and *Yahoo! News* On January 8, 2020, citing several industry sources.[110] The NCA report explained how Dustman had compromised an organization with which the NCA had "heavy involvement," revealed by *ZDNet* on January 9 to be the Bahraini national oil company,

106 We do not include Iranian claims of a cyber operation against U.S. defenses during the acknowledged missile attacks against U.S. bases in Iraq on 9 January, as there is no independent evidence that such operations occurred. Radio Farda, "Iran Disabled U.S. Monitoring Systems During Missile Attack, IRGC Commander Claims," *RFE/RL*, January 9, 2020, https://en.radiofarda.com/a/iran-disabled-us-monitoring-systems-during-missile-attack-irgc-commander-claims-/30368664.html.

107 Department of Justice, "Two Alleged Hackers Charged with Defacing Websites Following Killing of Qasem Soleimani," U.S. Department of Justice Office of Public Affairs, September 15, 2020, https://www.justice.gov/opa/pr/two-alleged-hackers-charged-defacing-websites-following-killing-qasem-soleimani.

108 Levi Gundert, Sanil Chohan, and Greg Lesnewich, "Iran's Hacker Hierarchy Exposed" (Recorded Future Insikt Group, May 9, 2018).

109 Saudi National Cybersecurity Authority, "Destructive Attack 'DUSTMAN': Technical Report" (Riyadh, December 2019).

110 Sean Lyngaas, "Saudi Cyber Authority Uncovers New Data-Wiping Malware, and Experts Suspect Iran Is behind It," *CyberScoop*, January 8, 2020, https://www.cyberscoop.com/saudi-arabia-iran-cyberattack-soleimani/; Jenna McLaughlin, "Saudis Warn of New Destructive Cyberattack That Experts Tie to Iran," *Yahoo! News*, January 8, 2020, https://news.yahoo.com/days-before-suleimani-strike-saudis-warned-of-new-destructive-cyber-attack-013125981.html.

BAPCO.[111] The *ZDNet* reporter claimed that the wiping incident in which Dustman was discovered took place on December 29, 2019, four days before the strike on Suleimani. According to the NCA report, the Dustman deployment was significantly different to the Shamoon incidents in the previous section, as it was compiled and deployed "with urgency."

This event, although occurring at a pivotal point in U.S.-Iran escalation, is generally not treated as part of the exchanges leading to the strike on Suleimani throughout December 2019. The exception is the first *Yahoo! News* report on Dustman, which mooted the possibility that "the wiper was deployed as retaliation" on the same day as the December 29, 2019, U.S. strikes on militia bases. This possibility is tempered by signaling in the malware, which contained the message "down with bin Salman," and would have probably been directed at the U.S. rather than Saudi Arabia if designed as a response to these strikes.[112] A more likely assessment comes from the NCA report (also noted in the *Yahoo! News* and other coverage), suggesting that the wiper's urgency was a result of "multiple OPSEC failures" and wider industry reporting on Iranian wipers in December 2019.[113] In this interpretation, the wiper was deployed hastily because the threat actor was aware they had been detected and remediation was in progress. This assessment also raises the possibility that the minimal disruption experienced by BAPCO was not even the main purpose of the wiper. The threat actor may have mainly sought to erase all traces of their own activity on BAPCO networks, with any disruption and anti-Saudi signaling a side benefit.

111 Catalin Cimpanu, "New Iranian Data Wiper Malware Hits Bapco, Bahrain's National Oil Company," *ZDNet*, January 9, 2020, https://perma.cc/M3GV-ELRA; Dragos Inc., For an excellent discussion of an ICS-focused ransomware strain also pointing to a BAPCO compromise see "EKANS Ransomware and ICS Operations," February 3, 2020, https://perma.cc/9S7F-HXL7.

112 Insikt Group, "Iranian Cyber Response to Death of IRGC Head Would Likely Use Reported TTPs and Previous Access."

113 DUSTMAN had technical links to another wiper malware linked with Iranian MOIS-linked group APT34 by IBM. IBM Security, "New Destructive Wiper 'ZeroCleare' Targets Energy Sector in the Middle East" (IBM X-Force Incident Response and Intelligence Services (IRIS), January 2020).

Consequently, despite the "destructive" nature of the BAPCO incident, and its occurrence during escalated tensions, the threat intelligence industry—accurately, in our view—did not incorporate this incident into ongoing kinetic exchanges between the U.S. and Iran. The interpretive errors above did not lead analysts to build a tit-for-tat narrative around the BAPCO incident, suggesting that collaboration and open communication can help to avoid such errors.

Despite the "destructive" nature of the BAPCO incident, and its occurrence during escalated tensions, the threat intelligence industry—accurately, in our view—did not incorporate this incident into ongoing kinetic exchanges between the U.S. and Iran.

The Broader Regional Context

As well as considering the detail of specific incidents, unfulfilled expectations of an Iranian cyber response to the Suleimani killing must be placed in a broader domestic and regional context. While it is beyond the scope of this paper to consider these issues in detail, wider factors influence the strategic understanding of cyber operations just as much as the detailed capabilities discussed above, in three distinct ways.

First, any Iranian response—cyber or otherwise—had to consider the risk of further international isolation. After the strike that killed Suleimani, the world's attention was focused on how Iran would respond. The international response to U.S. action was mainly rhetorical with little associated action—notwithstanding the UN report cited above. Many key international players urged de-escalation. By de-escalating and reacting proportionately, Iran could be seen as a responsible player, potentially gaining diplomatic advantage for the regime. Further Iranian action likely would not have caused any backlash from China or Russia, but it would have risked punitive measures from the European Union, who sought to provide some level of relief from the Trump administration's "maximum pressure" campaign and to dampen his volatile messaging on Iran. If Iran escalated further, including through cyber means, they would provide the U.S. justification to cause even greater harm to the Iranian economy

and potentially cause a return to the pre-JCPOA unified international sanctions regime that severely damaged their economy, especially given Trump's foreign policy volatility. More widely, Iran has a breadth of foreign policy concerns, such as potential upcoming nuclear talks, the region's gradual normalization of diplomatic ties with Israel, and delicate relationships with the Gulf states, all of which factor into calculations of response just as much as proportionality.

Iran has a breadth of foreign policy concerns, such as potential upcoming nuclear talks, the region's gradual normalization of diplomatic ties with Israel, and delicate relationships with the Gulf states, all of which factor into calculations of response just as much as proportionality.

Second, from a domestic perspective, the Iranian response navigated a difficult economic situation and highly combative domestic politics. In the two months preceding the Suleimani killing, there were some of the most substantial protests in the Islamic Republic's history. The unrest began when the government tripled gasoline prices in an attempt to reduce their budget deficit. Protesters burned banks, police stations, symbols of the Revolution, and other symbols of the regime's power. In response, security forces unleashed a violent crackdown and shut the country's internet down for a week. This period of unrest became known as Bloody November, and Iranian security forces killed at least 304 protesters.[114] In contrast, most of the interlude between January 3 and January 8, 2020, saw public displays of solidarity and mass attendance at the funeral of and demonstrations for Suleimani.[115] Choosing not to escalate beyond missile strikes may have been a strategic decision to capitalize on the drastic swing from the Bloody November unrest to national unity following the Suleimani killing.

Third, on January 8, 2020, an Iranian air defense unit shot down a Ukraine Air passenger jet, killing 176 passengers, many of whom were not from

114 Human Rights Watch. "Iran: No Justice for Bloody 2019 Crackdown," November 17, 2020. https://www.hrw.org/news/2020/11/17/iran-no-justice-bloody-2019-crackdown.

115 Guardian News. *Massive Crowds Attend Funeral Processions as Suleimani's Body Returned to Iran*, 2020. https://www.youtube.com/watch?v=-x88HVir4qA. These were likely orchestrated by the regime, at least in part.

Iran.[116] The international backlash was substantial, exacerbated by Iran initially refusing to admit the plane was shot down.[117] The response ultimately culminated in an immediate call for an investigation and Canada, Afghanistan, Sweden, Ukraine, and the United Kingdom signing a memorandum of understanding demanding full reparations from Iran.[118] Iranian protesters once again returned to the streets to protest the regime in the wake of the Ukraine Air incident, highlighting the volatility of domestic regime support. This chance incident would undoubtedly also have affected Iranian decisions over the risks of any further response to the Suleimani killing.

These three factors compound the complexity of Iranian decision-making following the Suleimani killing. They add to the issues of capacity and direction discussed in Section 2, including the residual impact of the 2019 leaks that forced several Iranian cyber actors to rebuild their offensive capabilities, and the thin spread of cyber resources across internal and interstate objectives. While this review of such broader factors is necessarily brief, it highlights how cyber operations are conducted within specific regional and domestic contexts. The repressive character of Iranian domestic politics, as well as its fluid and militarized regional context, prevented simple tit-for-tat calculations in responding to the Suleimani killing overall, as well as the inclusion of cyber capabilities to any response.

116 "Canada's Response to Ukraine International Airlines Flight PS752 Tragedy." Accessed April 8, 2021. https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/flight-vol-ps752.aspx?lang=eng.

117 This backlash contrasted starkly with the response to the USS Vincennes incident during the Iran-Iraq War. During the Iran-Iraq War in 1988, the USS Vincennes mistook an Iranian airliner for a military aircraft and shot it down. That airliner had 290 civilians onboard. Iran expected the response to such an event to be substantial, but the international community said and did very little. That muted response left Iran with a sense of isolation which expedited the agreement of an Iran-Iraq ceasefire. Ghattas, Kim. *Black Wave: Saudi Arabia, Iran, and the Forty-Year Rivalry That Unraveled Culture, Religion, and Collective Memory in the Middle East*. First. New York: Henry Holt and Company, 2020, 178.

118 Canada, Global Affairs. "Backgrounder—Memorandum of Understanding on Cooperation Regarding Negotiations on Reparations by Iran." Backgrounders. gcnws, July 2, 2020. https://www.canada.ca/en/global-affairs/news/2020/07/backgrounder---memorandum-of-understanding-on-cooperation-regarding-negotiations-on-reparations-by-iran.html.

Conclusion

This paper has explored U.S. expectations and reality of Iranian cyber operations, both in longer-term trends and in a detailed case study around the killing of Qassem Suleimani. It has argued that U.S. expectations contain two key interpretive errors, at least in the public discourses available to researchers.

First, these expectations rely on early formative events to infer a continued disruptive and destructive Iranian cyber threat to the U.S. While Iranian threat actors have continued to deploy wipers and have sought to design—but not, as far as we are aware, successfully deploy—ICS malware against regional targets, the expectation that they would deploy these in a reactive, even irrational, manner against U.S. networks is based on incidents that have receded into what, in the fast-paced evolution of cyber strategy, is an increasingly distant past.

Second, U.S. expectations are at risk of mirror-imaging: assuming that Iranian cyber actors perceive the benefits and limitations of cyber operations in the same way as the U.S. defense and intelligence communities. This mirror-imaging is clearest in the U.S. characterization of cyber operations as a de-escalatory, proportionate response to kinetic strikes. However, mirror-imaging is also a danger for more sophisticated understandings of Iranian cyber operations based around persistent engagement. While Iranian actors have clearly embraced cyber-espionage campaigns for both strategic advantage and transnational repression, punctuated by disruptive wipers and ransomware, it is not clear that they would necessarily perceive U.S. actions to "defend forward" as the development of "agreed competition" or a new norm in this space.

Given these findings, this paper makes several policy recommendations, seeking to assist the extensive investment across public and private sectors to counter Iranian offensive cyber operations, helping them to avoid the interpretive errors above. The overall goal is to view Iranian actors as

rational participants in geopolitical cyber competition, rather than reactive and often irrational adversaries. Whether the COVID-19 pandemic, which has hit Iran harder than many surrounding states, has affected its cyber strategy is difficult to tell. But initial indications suggest that, like many other states, Iran has prioritized pharmaceutical and healthcare targets for cyber espionage, as well as suffering from a significant decrease in available human and technical resources. The change in perspective advocated by this paper takes our understanding of Iranian cyber strategy beyond tit-for-tat, enabling both companies and government actors to prepare better for any future increase in tensions, especially in the context of the new Iranian President, ongoing nuclear negotiations, and a pandemic-influenced digital world.

Policy Recommendations

1) Analytically situate Iranian cyber operations in their regional geo-political context. Cybersecurity analysts should prioritize understanding the domestic and regional context of Iranian cyber campaigns, especially pressures on Iranian leadership from domestic unrest and regional proxy conflicts, as well as the use of cyber capabilities for transnational repression. Iranian cyber operations should be treated as non-dyadic, often improvisatory, and flexible campaigns that fulfil multiple strategic goals with constrained resources, rather than specific disruptive responses to adversary actions.

2) Work closely with regional partners, especially in the Gulf, to improve cyber defenses. U.S. government and industry actors should work closely with their allies and partners to improve cyber defenses across the board, especially in the Gulf states and in critical infrastructure sectors, as Iranian offensive cyber operations are likely to flexibly select targets based on ease of access. Many Gulf states have become regional centers for cybersecurity, and so the U.S. should further assist these states to act as leaders in improving cyber defenses across the region. This work should focus on Gulf government leverage over private sectors as part of national plans to embrace technology-driven economies, and emphasize the importance of regional cooperation in both incident response and supply chain protection.

3) Carefully consider Iranian interpretation of U.S. and allied offensive cyber operations. The U.S. view of cyber operations as a less escalatory form of retaliation may not be shared by Iranian targets of such operations, despite explicit signaling of this intent. More specifically, Iranian actors are unlikely to distinguish sharply between U.S. "reactive" offensive cyber operations designed to communicate red lines on the one hand, and an ongoing broader range of cyber-espionage and tactical disruption by both the U.S. and allies on the other, especially where offensive operations technically rely on these broader accesses. If retaliatory cyber operations do not function as clear signals, they may be better avoided.

4) Link offensive cyber operations closely to international law. Iran's rhetoric in international cybersecurity governance forums indicates a willingness to apply international legal concepts to cyber operations, including issues of sovereignty, use of force, and attribution. The U.S. and other states can help encourage such application by explicitly justifying their own cyber operations under specific elements of international law, rather than in less precise terms around national or regional security. This would clarify dominant interpretation of international law as applied to cyber operations for Iran, as well as developing a body of state practice that encourages responsible state behavior more broadly.

5) Explore the potential for dialogue to establish shared understanding. Incorporating cyber operations into (indirect) U.S.-Iran diplomacy is challenging in the context of difficult nuclear negotiations, where Iran seeks to keep other regional security issues off the table. However, the U.S. government should explore possibilities for dialogue through other channels, as well as cooperation on internationally recommended confidence-building measures for cybersecurity. The analysis in this paper is limited, and there is much further work to do to gain a sufficient understanding of Iranian cyber strategy and practice.

Appendix

Table 1 below provides a numeric overview of the dataset underlying this paper, with several important limitations. First, it is not a complete list of all cyber activity linked to Iran, although it does include most notable activity in public reporting. Second, the category of "cyber response" denotes a reported connection to earlier cyber and/or non-cyber incidents even though these connections are often inaccurate or overstated, leading to the tit-for-tat narrative that is the main focus of this paper. Third, as discussed in Section 2, the "incident" framing of this table can be unhelpful, artificially separating specific compromises from wider campaigns, toolsets, and threat actors. Finally, all incidents in this table are counted from date of first report, so multiyear campaigns are only included once. The dataset and its sources are discussed further in Section 2.

Table 1: Overview of Iran-Related Cyber Activity

Year	Total incidents	Incidents targeting Iran	Incidents attributed to Iran	Cyber responses*
2009	2	0	2	0
2010	3	1	2	0
2011	2	0	2	0
2012	8	2	6	3
2013	5	1	4	0
2014	3	0	3	1
2015	6	0	6	1
2016	1	0	1	0
2017	6	0	6	0
2018	7	1	6	1
2019	16	3	13	2
2020	21	5	16	3
Total	80	13	67	11

Table 2: Selected U.S. Legal Action against Iranian Individuals and Entities for Alleged Cyber Activity

Date unsealed	Type (FBI office/ other org)	Subject	Reason
March 24, 2016	Indictment (New York)	Seven individuals for ITSecTeam and Mersad (IRGC)	DDoS attacks against U.S. financial sector, Bowman dam intrusion
July 17, 2017	Indictment (Vermont, New York)	Two individuals, no public state connection	Historic software export violation (ArrowTech), third individual pardoned in JCPOA negotiations
November 21, 2017	Indictment (New York)	One individual, previous work with "Iranian military"	Hack-and-leak of HBO
March 23, 2018	Indictment (New York)	Nine individuals working for the Mabna Institute (IRGC)	Data exfiltration from companies, universities worldwide
March 23, 2018	Sanctions (Treasury)	Ten individuals and one entity (Mabna Institute)	" "
November 28, 2018	Indictment (New Jersey)	Two individuals, no public state connection	Samsam ransomware
February 13, 2019	Indictment (Washington)	Four individuals working for IRGC	Social engineering and malware targeting U.S. defense personnel
February 13, 2019	Sanctions (Treasury)	Net Peygard Samavat company (MOIS and IRGC)	" "
September 15, 2020	Indictment (Boston)	Two individuals in Iran and Palestine, no state connection	Website defacement following killing of Qassem Suleimani
September 17, 2020	Indictment (Virginia)	Three individuals (IRGC)	Data exfiltration from aerospace and defense companies
September 17, 2020	Sanctions (Treasury)	45 individuals and Rana Institute (MOIS)	Malware campaign against dissidents and opposition
October 7, 2020	Seizure (DoJ under FARA)	92 domain names associated with disinformation campaign	Associated with disinformation operation during U.S. elections

Cyber Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/Cyber