How Does Iran Conceive of Cyber as Part of its National Strategy?

Alex Campbell, CJ Dixon, Gussie Gronquist, Tala Haikal, Matthew Kalin
Advisor: Professor Greg Rattray

For FireEye iSIGHT Threat Intelligence

May 7, 2019

TABLE OF CONTENTS

Executive Summary 3

Introduction 6

Research Methodology & Findings 7

Applying Strategic Culture to Iranian Cyber Employment 9

Future Scenarios 12

Conclusion & Recommendations 16

Addendum 19

EXECUTIVE SUMMARY

Iran remains perhaps the least-understood major threat actor facing the United States in cyberspace. Due to the constant engagement inherent to state computer network operations (CNO) from espionage to disruption, it is vital for US decision-makers to understand how their Iranian counterparts conceive of offensive CNO in order to avoid misperception and accidental escalation. Our report aims to answer the following research questions:

- How does Iranian strategic culture inform Iranian use of CNO?
- What discrepancies exist between the American and Iranian conceptions of cyber?
- Which directions might Iranian cyber activity take in the future?

Our research began by characterizing Iranian strategic culture, which can be understood as the ingrained "ideas, conditioned emotional responses, and patterns of habitual behavior" shared within a community of national decision-makers and derived from that community's common experiences. Strategic culture helps explain why decision-makers in a given country view tools for the use of force, like CNO or nuclear weapons, differently than their counterparts elsewhere. As a characterization of Iranian strategic culture, we argue that Iranian decision-makers:

- prioritize regime security
- emphasize self-reliance
- orient conventional military forces towards defense
- pursue regional hegemony
- favor asymmetric means for projecting power

We then developed four scenarios occurring over the next three years based on 1) our understanding of Iranian strategic culture and 2) our understanding of key drivers of Iranian behavior *independent* of strategic culture, which are listed below:

- regime stability
- regional power dynamics
- domestic power dynamics
- economic fragility
- US policy towards Iran

We designed scenarios by imagining different possible conditions for each of these drivers, then using our characterization of Iranian strategic culture to play out how Iranian decision-makers would likely react to these stimuli. Developing scenarios helps clarify our analytical assumptions while outlining what we consider to be the most salient implications for US decision-makers.

Scenario 1: It's Still the Economy, Stupid

Context: Continued sanctions and European withdrawal from the JCPOA exacerbate Iran's economic fragility, hurting both ordinary citizens and government revenues. Economic grievances drive broad-based protests against the government.
Signposts: Sharp declines in GDP, employment; short-term attempts to mitigate discontent (e.g. government salary increases); Iranian diplomatic entreaties to US and allies
Predicted Iranian behavior: Iran increases espionage and offensive CNO against sanctions implementers abroad and dissidents at home.
Key findings: *If the US continues to push for an Iranian economic collapse, Iran will lash out more vigorously against the US and any allies.*

Scenario 2: A More Hardline Iran

Context: The IRGC cements control over Iranian domestic institutions as Mohammad Baqr Qalibaf wins the 2021 presidential election and a pliant Ebrahim Raisi succeeds Khamenei.
Signposts: IRGC candidates perform well in 2020 legislative elections; more resignations from Rouhani administration (e.g. Zarif); political/military leadership reshuffling (e.g. Salami)
Predicted Iranian behavior: Iran's foreign policy becomes centralized under the IRGC, characterized by more aggressive CNO and information operations against regional adversaries.
Key findings: *The Supreme Leader has neither a monopoly on decision-making nor the influence to check the IRGC; decentralized Iranian decision-making engenders misperception but so would greater IRGC influence.*

Scenario 3: A Blue White House

Context: A Democrat wins the US 2020 presidential election and rejoins the JCPOA without preconditions.
Signposts: Candidates' rhetoric emphasizes rapprochement with Iran; Obama Iran policy alumni join new administration; Iran maintains JCPOA status quo
Predicted Iranian behavior: Iran decreases offensive CNO against the US and its allies, but continues espionage and capability development.
Key findings: *US-Iran relations transcend the JCPOA, and provocative Iranian behavior such as increasingly sophisticated espionage will persist regardless of the deal's status.*

Scenario 4: Doom and Gloom

Context: With Iran poised for a nuclear breakout, the US, Israel, and Saudi Arabia conduct a joint CNO disrupting multiple Iranian critical infrastructure sectors. US rhetoric advocates military action for regime change.
Signposts: Hardliners win 2020 and 2021 Iranian elections; US discourse (op-eds, think tanks) argue more for war with Iran; EU's INSTEX workaround fails to improve Iran's economy
Predicted Iranian behavior: Iran retaliates with offensive CNO against the US energy sector, causing significant physical damage to a nuclear power plant and loss of life.
Key findings: *Iran fears regime change above all and will act without restraint given a credible threat; the US underestimates Iranian cyber capabilities; the US would likely go to war if hit with a destructive state-sponsored CNO.*

In conclusion, we recommend the following actions for US policymakers.

- **Continue indicting Iranian hackers.** Even if it does not alter Iranian behavior, clearly and consistently establishing what the US considers illegal behavior helps mitigate misperception and unintended escalation. Indictments further deter and isolate individual hackers who participate in the pseudo-capitalist hacker ecosystem (PCHE) but are not part of the establishment by limiting travel and economic opportunities abroad.

- **Maintain dialogue through Track 2 diplomacy.** From a US perspective, the opacity of Iranian decision-making makes dialogue at some level essential to understanding Iranian priorities. In its absence, long-standing enmity is likely to cause both states to overestimate the threat posed by the other. Furthermore, having access to the US (and therefore to the hope of sanctions alleviation) lends clout to reformist, moderate voices in Iran in internal disputes with hardline factions.

- **Engage early with allies and competitors.** Any effective policy to coerce, deter, or negotiate with Iran needs buy-in from US regional allies and competitors, or at least tacit agreement to not act as a spoiler. Specifically, the US should engage early with Israel, the GCC, the EU, Russia, China, and India. Iran overestimates the degree of cohesion among its adversaries, so more aggressive actions taken by Saudi Arabia or Israel will nonetheless be associated with the US. Coordination with European and other allies is also important, but Israel and the GCC are more likely to unilaterally escalate against Iran with the expectation of US support. As major Iranian trading partners, Russia, China, and India should also be engaged to ensure they do not obstruct potential US policies.

- **Harden defenses around critical infrastructure.** Recent operations like the wave of DNS hijacking show that Iranian actors' toolkits continue to evolve. Expectations of future attacks should therefore not be limited to past Iranian targets or TTPs (tactics, techniques, and procedures).

INTRODUCTION

The US withdrawal from the Joint Comprehensive Plan of Action (JCPOA) on May 8th, 2018 marked an inflection point in US-Iran relations. As a result, the frequency and nature of offensive computer network operations (CNO) originating in Iran are also expected to shift. To better prepare US decision-makers in the public and private sectors for these shifts, this report attempts to answer the following three research questions: How does Iranian strategic culture inform Iranian use of cyber network operations? What discrepancies exist between the American and Iranian conceptions of cyber? Which directions might Iranian cyber activity take in the future?

Our report focuses on the concept of strategic culture as a means to understand Iranian decision-making. Jack Snyder defines strategic culture as “the sum total of ideas, conditioned emotional responses, and patterns of habitual behavior that members of a national strategic community have acquired through instruction or imitation and share with each other.”[1] In other words, strategic culture influences policy at a deeper, more psychological level than doctrine or strategy by limiting the scope of what decision-makers consider to be valid options regarding the use of force in international affairs. Understanding strategic culture provides insight into the decisions of states by creating a model for national decision-making through which to examine various scenarios. In the context of this report, defining Iranian strategic culture facilitates more accurate answers to the research questions above. Strategic cultures differ across nations, and help explain why policymakers in Iran and the US faced with the same disruptive technology and same scenarios can view them differently.

[1] Snyder, *The Soviet Strategic Culture*, p. 8.

The second section of this report summarizes the research methodology and findings. The third section provides an analysis of the proposed model of Iranian strategic culture, as well as its application to cyber employment. The fourth section outlines the future scenarios used to systematically examine Iranian cyber activity under varying international and domestic conditions. Finally, the fifth section of this report concludes with the implications of our analysis, as well as the resulting recommendations for US policymakers.

RESEARCH METHODOLOGY & FINDINGS

Our research methodology comprised desktop research and a literature review, interviews of experts, and analysis of open-source data on the frequency and targets of attributed Iranian offensive CNO.[2] Through this, we identified key elements of Iran's decision-making, use-of-force context, and cyber employment and capability to define a model of Iranian strategic culture and cyber strategic culture. The resultant models of strategic culture served as the basis of our scenario development and recommendations.

The nature of available information on Iran limited our research methodology and scope. First-hand data collection through travel was not feasible, as was a fair amount of Internet-based primary source research due to domestic Iranian Internet controls. Furthermore, many accessible primary sources were official Iranian government translations and not translated independently by the team. Therefore, we chose a more theoretical, deductive approach.

[2] See Addendum for list of experts interviewed.

Our examination of Iranian geography, history, society, demographics, culture, religion, and politics produced our understanding of Iranian strategic culture. The following five trends characterize Iranian national strategic culture:

- Prioritizing regime security
- Emphasizing self-reliance
- Orienting conventional military forces towards defense
- Pursuing regional hegemony
- Projecting national power through asymmetric means

We believe these five characteristics describe the strategic culture influencing Iranian national decision-makers. However, the process of creating policy in Iran is fractured, driven by the competitive nature and low level of institutionalization of Iranian government organizations. In practice, this means that different areas of Iranian foreign policy are overseen by different factions who seize and protect jurisdictions based on relative power shifts. Institutions generally lack entrenched interests, instead representing arenas for contestation between political factions that then wield them against rivals.

Importantly, we conceptualize strategic culture as only one input into strategic decision-making in Iran. Like decision-makers anywhere, Iranian leaders make choices in reaction to stimuli and with consideration to standing policy or doctrine. However, strategic culture constitutes the lens coloring how Iranian decision-makers perceive a given stimulus, and which operational approach they choose to employ in response.

The relevant bodies for conducting CNO are primarily the Islamic Revolutionary Guards Corps (IRGC) and Ministry of Intelligence (MOIS). The key decision-makers in Iranian foreign policy writ large include the IRGC, MOIS, Supreme Leader Ali Khamenei, and a small number of politicians at the presidential or cabinet level. In contrast, the Iranian Army (Artesh), Ministry of Foreign Affairs (MFA), and other elected officials play significantly subordinated roles in foreign policy.

APPLYING STRATEGIC CULTURE TO IRANIAN CYBER EMPLOYMENT

We also sought to define the cyber-specific element of Iranian strategic culture. Through examining behavior of various known Iranian advanced persistent threat (APT) groups and reviewing Iran-attributed cyber network operations, we define Iranian cyber strategic culture as:

- Seeking information for strategic advantage
- Perceived victimhood, therefore retaliatory behavior
- Use of cyber as a pillar of deterrence
- Executed by a pseudo-capitalist hacker ecosystem rather than official military assets

Seeking information for strategic advantage: Offensive CNO has become a core tool of Iranian statecraft, but is used most often to conduct traditional espionage against regional rivals and perceived domestic threats. An analysis of 62 open-source reports reveal that 73% of cyber operations attributable to Iran can be classified as espionage.[3] The Iranian government is primarily concerned with the survival of the current regime and the Islamic Revolution. According to the concept of "expediency of the regime" and in contrast to inflammatory public rhetoric, Iran typically adopts a pragmatic approach to regime survival in all domains of conflict. [4] In cyberspace this behavior translates to CNO for traditional intelligence collection to gain strategic advantage. For example, IRGC-affiliated hackers allegedly stole research, proprietary data, and intellectual property from hundreds of universities and global institutions.[5]

[3] Council on Foreign Relations. *Cyber Operations Tracker* available at: https://www.cfr.org/interactive/cyber-operations/search?keys=Iran

[4] https://www.washingtoninstitute.org/uploads/Documents/pubs/MESM_7_Eisenstadt.pdf

[5]https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary

Perceived victimhood, therefore retaliatory behavior: Iran has demonstrated the capacity for high-profile and destructive cyber attacks, but has typically conducted cyber attacks in response to perceived aggression. Iran considers itself to be the victim in the international arena and responds with what it perceives to be proportional responses to aggression. In 2012, a hacker group calling itself the Izz ad-Din al-Qassim Cyber Fighters launched a massive distributed denial of service (DDoS) attack against US financial institutions. US intelligence assessed that the attack was in response to sanctions imposed on the Iranian government for its nuclear weapons program.[6] Iran likely perceived the DDoS attack as a proportional response in a dispute with an adversary, targeting the US financial system to retaliate against sanctions blocking Iran from the global financial system. The 2014 attack on the Sands Las Vegas Corporation, months after CEO Sheldon Adelson called for a nuclear strike against Iran, represents a similar tit-for-tat response.[7]

Use of cyber as a pillar of deterrence: Iran CNO against Western states will often focus on individuals and institutions involved in the development and implementation of policy towards Iran, with offensive actions aiming to deter behavior detrimental to Iran. Iran, like any other state, values intelligence that will provide strategic advantage. According to the Associated Press and data provided by Certfa, Iran attempted to hack the email accounts of US Treasury officials and think tank employees as well as supporters, critics, and enforcers of the original JCPOA.[8] It can be surmised that Iranian actors attempted to access these emails to gain insight into pending sanctions.

[6] https://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html

[7] https://www.recordedfuture.com/iran-hacker-hierarchy/

[8] https://hillreporter.com/iranian-state-affiliated-hacker-group-targeted-13-us-treasury-officials-17813

Executed by a pseudo-capitalist hacker ecosystem rather than official military assets: Iran utilizes a pseudo-capitalistic ecosystem of contractors to quickly conduct CNO. This strategy is consistent with Iran's broader strategic preference for proxies, which afford Iran deniability and allow it to maintain a narrative of victimhood. Iran also uses proxies out of necessity, since its government lacks the capital and institutional knowledge necessary to maintain official cyber assets. Using proxies enables Iran to rapidly bring cyber assets to bear against an adversary, but can also have unintended consequences: overreach by Iranian Cyber Army proxies led to the 2010 "Sino-Iranian Hacker War," which saw retaliatory defacement of Iranian websites by Chinese patriotic hackers.[9]

Iran's proxy ecosystem consists of contractors hired to conduct CNO on behalf of Iranian government bodies, principally the IRGC and MOIS. Hackers responsible for CNO against everything from the US Justice Department, US financial institutions, and Saudi Aramco have been tied to the IRGC. Conversely, recent disclosures appear to link APT34/Oilrig to the MOIS. [10] The IRGC and MOIS set objectives, choose targets, and then commission these private contractors to execute operations. A campaign will often be subdivided among different contractors, both because the Iranian government trusts contractors less than uniformed personnel and because contractors often lack the capacity to take on a project alone.[11] Operations whose strategic purpose requires rapid execution often drive the Iranian government to delegate a greater share to contractors, creating a risk of accidental escalation. Examples of such operations include rapid retaliatory strikes like the 2012 DDoS of US financial institutions and the 2014 Sands Las Vegas attack.

[9] https://www.theguardian.com/technology/2010/jan/12/iranian-hackers-chinese-search-engine
[10] https://www.wired.com/story/iran-hackers-oilrig-read-my-lips/
[11] https://carnegieendowment.org/2018/01/04/iran-s-cyber-ecosystem-who-are-threat-actors-pub-75140

These contractors often share code libraries, individual employees, and TTPs. When combined with the often unclear relationship between contractors and official Iranian government bodies, shared TTPs can contribute to escalation by obscuring attribution. For example, an accidentally escalatory attack by an Iranian contractor could be mistakenly attributed to a different group acting under more direct Iranian government control. Iranian hackers also commit freelance criminal fraud when not on government contract.[12] The fact that both criminal and government-directed CNO originating from Iran against private sector targets are committed by the same individuals further complicates questions of attribution and purpose. The unofficial status of these contractors creates both problems and opportunities from the US perspective: US sanctions against Iranian government bodies like the IRGC will not directly affect contractors, but the fact that contractors are often less ideological and may desire a life outside of Iran makes them more susceptible to individual indictments and travel bans that drive a wedge between them and their government employers.

FUTURE SCENARIOS

After establishing a baseline of knowledge about Iranian history and strategic culture, decision-makers, cyber background and capabilities, and American perceptions of Iran, we developed four future scenarios in order to systematically examine Iranian cyber activity under varying international and domestic geopolitical conditions. This approach is based on the scenario planning method described by futurist Peter Schwartz in his book *The Art of the Long View: Planning for the Future in an Uncertain World*.

[12] https://carnegieendowment.org/2018/01/04/iran-s-cyber-ecosystem-who-are-threat-actors-pub-75140

Schwartz explains that “the scenario process provides a context for thinking clearly about the impossibly complex array of factors that affect any decision…thinking through these stories, and talking in depth about their implications, brings each person’s unspoken assumptions about the future to the surface. Scenarios are thus the most powerful vehicles I know for challenging our ‘mental models’ about the world, and lifting the ‘blinders’ that limit our creativity and resourcefulness.”[13] The scenario process provides a systematic way to examine multiple, plausible futures through well-researched stories, which are “oriented toward real-life decisions and designed to bring forward surprises and unexpected leaps of understanding.”[14]

Essential to the scenario process is first identifying the key drivers and main factors which influence each scenario. We established the following key drivers present in all four scenarios:

- Iranian regime stability and survival
- Regional power dynamics
- Domestic power dynamics
- Iran’s economic fragility
- US policy toward Iran

The first scenario, “It’s Still the Economy, Stupid,” focuses on Iran’s economic fragility as economic hardship will draw attention to the need for major economic and political reforms within the country. We consider this highly likely within the next three years. In this scenario, Iran may stop abiding by the terms of the JCPOA following the collapse of INSTEX and subsequent European withdrawal from the deal. Increased international isolation of Iran will further contribute to the country’s economic downturn. Specific signposts indicating realization of this scenario include worsening macroeconomic indicators like GDP and employment, broad

[13] Schwartz, *The Art of the Long View*, pp. xiv-xv.
[14] Ibid., p. xiii.

economically-motivated protests outside of major cities, harsher US sanctions and rhetoric (e.g. the recent FTO designation of the IRGC), short-term Iranian efforts to placate citizens (e.g. increased government salaries), and Iranian efforts to resume negotiations or backchannels with the US. Under these circumstances, Iran is likely to expand its cyber espionage activities as its relations with Western powers worsen. Overall, CNO against governments (and private sector organizations) implementing sanctions will increase, as well as cyber crime for financial gain. The most salient insight from this scenario is that an Iranian economic collapse would likely produce more aggressive cyber operations against the US and its allies.

The second scenario, “A More Hardline Iran,” identifies Ebrahim Raisi as the successor of Supreme Leader Ayatollah Ali Khamenei and Mohammad Baqr Qalibaf as Iran’s next president. Both individuals support the Guards’ ideology and protect its economic interests. We have moderate-to-high confidence in this scenario occurring, with the following signposts indicating its realization: hardliner victories in the 2020 Iranian legislative elections, more resignations from Rouhani administration officials, and reshuffling of military leadership (e.g. the new IRGC chief Salami) towards more hardline voices. This scenario suggests that the new Supreme Leader does not have the power or ability to check the power of the IRGC. In addition, an IRGC-dominated cabinet is likely to consolidate Iranian foreign policy and decision-making. Under these conditions, there will be an uptick in domestic usage of cyber (consolidating domestic power and cracking down on dissent and opposition), an uptick in regional usage of cyber, and an uptick in informational warfare and propaganda. The most salient insight here is that more centralized Iranian leadership, especially under the Guards, would be more assertive abroad (including using CNO). While more centralized decision-making would aid communication, greater IRGC influence would also engender misperception due to the organization's opacity.

The third scenario, "A Blue White House," assumes a Democratic victory in the 2020 US presidential election and stipulates that the future US president will rejoin the JCPOA without any preconditions. We see this scenario as moderately plausible, and forecast the following signposts to indicate its realization: campaign rhetoric prioritizing rapprochement with Iran, Obama Iran alumni joining the new administration, and an openness to negotiate from Iran. This scenario could result in a decrease in Iranian CNO against the US and its allies. However, Iran will likely continue to build up its cyber capabilities and prioritize espionage and less disruptive attacks. Iranian strategic culture so favors the low-cost, asymmetric, relatively deniable characteristics of CNO that it will pursue capability development regardless of a US-Iran rapprochement.

The fourth scenario, "Doom and Gloom," suggests Iran is poised for a nuclear breakout and in response the US, Israel, and Saudi Arabia will launch a joint CNO against Iran's critical infrastructure with the threat of follow-on conventional military action. We consider this scenario unlikely, but consider the following signposts evidence of its realization: Iran restarting its nuclear program, the EU's INSTEX workaround failing to improve Iran's economy, hardliner victories in the Iranian 2020 and 2021 elections, a "Green Revolution 2.0" occurring during Iran's 2021 elections, US public opinion (op-eds, think tanks) voicing support for war with Iran, and the US finalizing its nuclear technology transfer to Saudi Arabia. Overall, the rise of a strong Iranian opposition (that the US can support), a conservative US President in 2020, and the consolidation of power by Saudi Arabia's Crown Prince Mohammed bin Salman would also facilitate this future.

This scenario implies that Iran will not hold back and will respond by lashing out against the US and its allies using all means available. To clarify the consequences for US audiences, we imagined a successful Iranian CNO against a US nuclear power plant—reflecting our assessment of growing Iranian capability as well as Iran's preference for tit-for-tat attacks—producing significant destruction and loss of life.

These four scenarios provide a picture of Iran's future and should encourage discussion among American policymakers and aid strategic planning. These scenarios by themselves do not determine strategy any more than a forecast does. Thus, US policy towards Iran requires strategy in light of these scenarios.

CONCLUSION & RECOMMENDATIONS

Having developed a working understanding of Iranian strategic culture and four scenarios illustrating future avenues for Iranian cyber threat activity, we then outlined implications of this analysis for US decision-makers in the public and private sectors. We believe the following policies will help the US mitigate the damage done by Iranian cyber threat activity and avoid unintentional aggression.

- **Continue indicting Iranian hackers.** Even if it does not alter Iranian behavior, clearly and consistently establishing what the US considers illegal behavior helps mitigate misperception and unintended escalation. Indictments further deter and isolate individual hackers who participate in the pseudo-capitalist hacker ecosystem (PCHE) but are not part of the establishment by limiting travel and economic opportunities abroad.

- **Maintain dialogue through Track 2 diplomacy.** From a US perspective, the opacity of Iranian decision-making makes dialogue at some level essential to understanding Iranian priorities. In its absence, long-standing enmity is likely to cause both states to overestimate the threat posed by the other. Furthermore, having access to the US (and therefore to the hope of sanctions alleviation) lends clout to reformist, moderate voices in Iran in internal disputes with hardline factions.
- **Engage early with allies and competitors.** Any effective policy to coerce, deter, or negotiate with Iran needs buy-in from US regional allies and competitors, or at least tacit agreement to not act as a spoiler. Specifically, the US should engage early with Israel, the GCC, the EU, Russia, China, and India. Iran overestimates the degree of cohesion among its adversaries, so more aggressive actions taken by Saudi Arabia or Israel will nonetheless be associated with the US. Coordination with European and other allies is also important, but Israel and the GCC are more likely to unilaterally escalate against Iran with the expectation of US support. As major Iranian trading partners, Russia, China, and India should be engaged to ensure they do not obstruct potential US policies.
- **Harden defenses around critical infrastructure.** Recent operations like the wave of DNS hijacking show that Iranian actors' toolkits continue to evolve. Expectations of future attacks should therefore not be limited to past Iranian targets or TTPs (tactics, techniques, and procedures).

This report has revealed a number of interesting areas for future research. Given the nature of Iran's pseudo-capitalist hacker ecosystem (PCHE), the US must determine how to dismantle irregulars in order to get strategic clarity on the regime's intent. Since the PCHE is often physically integrated with civilian institutions, one future research question might be: How should the US pre-position itself against an Iranian university computer science department? Or more broadly, how should the US pre-position its forces against Iranian civil society? Such future research should explore the ways in which US conventional forces can effectively target and dismantle Iranian civilian cyber forces without incurring excessive backlash from key allies.

Our research in this report characterizes Iran's behavior as extremely prone to escalation and misperception towards the US. As a country that adopts a wide definition of provocative behavior including the free flow of information, and acts with relatively little coordination or clarity in its retaliatory actions, Iran represents a difficult threat actor to anticipate or manage from the US perspective. Any decisions taken towards Iran must carefully weigh the gulf in perceptions between Iran and the US, as well as the history that has produced Iran's strategic culture.

ADDENDUM

We would like to thank the following scholars and practitioners for their guidance and expertise during this process:

- Erica D. Borghard, Adjunct Associate Research Scholar, Saltzman Institute of War and Peace Studies
- Annie Fixler, Deputy Director, Center on Cyber and Technology Innovation, FDD
- Jason Healey, Senior Research Scholar, SIPA
- James A. Lewis, Senior Vice President and Director, Technology Policy Program, CSIS
- Micah Loudermilk, Lead Associate at Booz Allen Hamilton (UAE)
- Afshin Molavi, Senior Fellow, SAIS Foreign Policy Institute
- Richard Nephew, Senior Research Scholar, SIPA
- Neal Pollard, Adjunct Associate Professor, SIPA
- Larry Potter, Adjunct Professor, SIPA
- Michael Singh, Managing Director, Washington Institute for Near East Policy