COLLIN ANDERSON + KARIM SADJADPOUR

IRAN'S CYBER THREAT

ESPIONAGE, SABOTAGE, AND REVENGE

COLLIN ANDERSON + KARIM SADJADPOUR

IRAN'S CYBER THREAT

ESPIONAGE, SABOTAGE, AND REVENGE

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: +1 202 483 7600
F: +1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org/pubs.

CONTENTS

ABOUT THE AUTHORS

COLLIN ANDERSON is a Washington, DC–based researcher focused on cybersecurity and internet regulation, with an emphasis on countries that restrict the free flow of information. Beginning in January 2018, he will be a fellow in the TechCongress Congressional Innovation Fellowship program. Prior to this fellowship, Anderson's involvements have included working as a researcher at Measurement Lab, producing numerous publications on privacy and security, and advising several organizations focused on human rights and Iran.

KARIM SADJADPOUR is a senior fellow at the Carnegie Endowment for International Peace, where he focuses on Iran and U.S. foreign policy toward the Middle East. He is also an adjunct professor at Georgetown University's School of Foreign Service, teaching a class on U.S. foreign policy and the Middle East.

ACKNOWLEDGMENTS

The authors would like to primarily thank Claudio Guarnieri, who was responsible for a significant amount of the technical analysis that informs this report.

Parts of this research were made possible based on the generous access to data provided by DomainTools. Similarly, this work was supported by dozens of organizations and individuals in the Iranian human rights community who provided cases and context, including but not limited to Amir Rashidi, Nariman Gharib, Nima Fatemi, Simin Kargar, and Farnoosh Hashemian.

In addition, Tim Maurer, Michele Dunne, Eli Levite, George Perkovich, Jen Psaki, and Mayss al-Alami at the Carnegie Endowment for International Peace, as well as former intern E. Scott Goldstein, provided very helpful feedback on drafts of the report.

Lastly, over the course of this research, we have had the fortune of meeting members of the cybersecurity and information technology communities that have acted as advisers and provided their expertise. It is immensely gratifying to know that behind the scenes of important communications platforms and security companies, there are people who hold such concern for the well-being of others in distant countries. These experiences have lent reassurance that the internet might continue to provide opportunities to at-risk populations against threats to their safety and liberty.

TIMELINE

JANUARY 1992
Iran first connects to the internet.

2000
Internet access becomes increasingly common, with hundreds of thousands of Iranians going online on a regular basis.

2001
The Supreme Council of the Cultural Revolution issues rules on internet access, including mandatory filtering and surveillance of sites considered politically, culturally, and religiously subversive.

FEBRUARY 2002
The hacking forum Ashiyane is created, serving as a catalyst for Iran's hacking community and later implicated in facilitating the Iranian government's repression of dissidents.

APRIL 2003
Sina Motalebi is arrested, one of the first bloggers in the world arrested for their online writings, commencing a crackdown on internet expression.

JUNE 2005
Hardliner Mahmoud Ahmadinejad is elected president of Iran, marking a new era of domestic repression and international hostility.

2007
Iranian threat actors begin to develop tools and conduct campaigns.

JUNE 2009
The contested reelection of Mahmoud Ahmadinejad provokes Iran's largest popular uprising since 1979, known as the Green Movement.

DECEMBER 2009
The Iranian Cyber Army defaces Twitter—taking it offline for several hours—in response to the Green Movement.

SEPTEMBER 2011
An Iranian hacker breaches Dutch security firm DigiNotar, allowing the Iranian government to spy on Gmail users in Iran. This remains one of the largest security breaches in the history of the internet.

APRIL 2012
Iranian oil infrastructure is targeted by sabotage malware agents Flame and Wiper.

JUNE 2012
New York Times reporter David Sanger makes public the details of Operation Olympic Games. One of the most sophisticated cyber attacks in history, the operation was begun by the United States and Israel in 2007 to covertly sabotage Iran's nuclear infrastructure.

JULY 2012
The Madi malware agent, the first Iranian-attributed espionage cyber campaign, is disclosed.

AUGUST 2012
Saudi Aramco, the world's largest oil company, has data destroyed by the malware agent Shamoon.

SEPTEMBER 2012
The first denial-of-service attacks against U.S. banks in what is known as Operation Ababil.

JUNE 2013
Pragmatic cleric Hassan Rouhani is elected president of Iran, with the promise of improving Iran's economy by resolving the nuclear standoff.

NOVEMBER 2013
Announcement of nuclear negotiations between the United States, China, Russia, UK, France, and Germany and Iran, resulting in an interim agreement.

JULY 2015
The nuclear deal is finalized, known as the Joint Comprehensive Plan of Action.

NOVEMBER 2016–JANUARY 2017
Cyber attacks against Saudi Arabia are renewed in Shamoon 2.

SUMMARY

Incidents involving Iran have been among the most sophisticated, costly, and consequential attacks in the history of the internet. The four-decade-long U.S.-Iran cold war has increasingly moved into cyberspace, and Tehran has been among the leading targets of uniquely invasive and destructive cyber operations by the United States and its allies. At the same time, Tehran has become increasingly adept at conducting cyber espionage and disruptive attacks against opponents at home and abroad, ranging from Iranian civil society organizations to governmental and commercial institutions in Israel, Saudi Arabia, and the United States.

IRAN'S CYBER THREAT ENVIRONMENT

- Offensive cyber operations have become a core tool of Iranian statecraft, providing Tehran less risky opportunities to gather information and retaliate against perceived enemies at home and abroad.
- Just as Iran uses proxies to project its regional power, Tehran often masks its cyber operations using proxies to maintain plausible deniability. Yet there are clear indications that such operations are conducted by Iranians and frequently can be linked to the country's security apparatus, namely the Ministry of Intelligence and Islamic Revolutionary Guard Corps.

- Iran's cyber capabilities appear to be indigenously developed, arising from local universities and hacking communities. This ecosystem is unique, involving diverse state-aligned operators with differing capabilities and affiliations. Over the decade that Iranians have been engaged in cyber operations, threat actors seemingly arise from nowhere and operate in a dedicated manner until their campaigns dissipate, often due to their discovery by researchers.
- Though Iran is generally perceived as a third-tier cyber power—lacking the capabilities of China, Russia, and the United States—it has effectively exploited the lack of preparedness of targets inside and outside Iran. Just as Russia's compromise of Democratic Party institutions during the 2016 U.S. presidential election demonstrated that information warfare can be conducted through basic tactics, Iran's simple means have exacted sometimes enormous political and financial costs on unsuspecting adversaries.
- The same Iranian actors responsible for espionage against the private sector also conduct surveillance of human rights defenders. These attacks on Iranian civil society often foreshadow the tactics and tools that will be employed against other targets and better describe the risks posed by Iranian cyberwarfare.
- Through technical forensics of cyber attacks, researchers documenting these campaigns can provide a unique window into the worldview and capabilities of Iran's security services and how it responds to a rapidly changing technological and geopolitical environment.

U.S. RESPONSES GOING FORWARD

- While Iran does not have a public strategic policy with respect to cyberspace, its history demonstrates a rationale for when and why it will engage in attacks. Iran uses its capabilities in response to domestic and international events. As conflict between Tehran and Washington subsided after the 2015 nuclear deal, so too did the cycle of disruptive attacks. However, Iran's decisionmaking process is obscured and its cyber capabilities are not controlled by the presidency, as evident in cases of intragovernmental hacking.
- The United States is reliant on an inadequately guarded cyberspace and should anticipate that future conflicts, online or offline, could trigger cyber attacks on U.S. infrastructure. The first priority should be to extend efforts to protect infrastructure and the public, including increased collaboration with regional partners and nongovernmental organizations targeted by Iran.

- Narrowly targeted sanctions could be used to deter foreign countries or other actors from providing assistance to Iranian offensive cyber operations. Such restrictions should still prioritize allowing Iranian society wide access to the internet and information technologies, to mitigate the regime's ability to control information and communications.
- The United States has pursued a name and shame strategy against Iranian threat actors, and should continue to do so. The Justice Department has issued indictments against Iranians implicated in disruptive campaigns and has successfully obtained the extradition from a third country of a hacker involved in the theft of military secrets. Because of the small operational footprint of the groups, targeted sanctions or legal proceedings are more symbolic than disruptive. These indictments may at least chill participation by talented individuals who wish to travel or emigrate.
- Iran continues to pursue its interests through cyber operations, engaging in attacks against its regional opponents and espionage against other foreign governments. A better understanding of the history and strategic rationale of Iran's cyber activities is critical to assessing Washington's broader cyberwarfare posture against adversaries, and prudent U.S. responses to future cyber threats from Iran and elsewhere.

INTRODUCTION

Cyberspace has become the newest frontier in the four-decade-long U.S.-Iran cold war. Perhaps more than any government in the world, the Islamic Republic of Iran has been the target of uniquely destructive cyber attacks by the United States and its allies. At the same time, groups associated with Iran's security forces—namely the Islamic Revolutionary Guard Corps (IRGC) and Ministry of Intelligence—have become increasingly adept at conducting their own offensive cyber operations. The targets of such operations include Iranian government critics at home and abroad, corporations, and nongovernmental organizations, as well as the economic, defense, and diplomatic institutions of countries including Germany, Israel, Saudi Arabia, and the United States.

The Iranian government has provided conflicting public accounts of its offensive cyber operations, touting its capabilities while denying responsibility for attacks attributed to it. Consistent with its use of proxy groups to assert its regional power, Tehran frequently masks its involvement in such operations using cutouts (intermediaries) to avoid attribution and provide it plausible deniability. Despite these denials, it is clear Iran has invested in indigenous cyber capabilities for both defensive and offensive purposes, and is willing to use them in the event of conflict.

Tehran's offensive cyber capabilities are relatively unsophisticated compared to states like China, Russia, and the United States. While the Iranian hacking scene emerged in the early 2000s, there is little evidence of state-aligned cyber activities before 2007. This comparatively late start and underinvestment in part accounts for its lower capacity. Yet Moscow's compromise of Democratic Party institutions and political operatives during the 2016 U.S.

election demonstrated that information warfare can be conducted through basic tactics. Iran has similarly preyed upon the lack of sophistication or preparedness of vulnerable targets both inside and outside Iran, including Saudi oil companies, Middle Eastern governments, and U.S. banks. Though these operations have often caused great financial damage, the methods used to destroy data or disrupt access were relatively simple.

Iran has demonstrated how militarily weaker countries can use offensive cyber operations to contend with more advanced adversaries. Tehran's operations against foreign interests have been mostly espionage and sabotage campaigns against soft targets in rival countries, rather than economic theft. Disruptive and destructive attacks have repeatedly been used by Tehran to signal its ability to impose retaliatory costs on its adversaries. Overall, these disruptive incidents appear to have been restrained based on strategic calculations, and limited to tit-for-tat exchanges within the same domain during times of conflict.

Iran has demonstrated how militarily weaker countries can use offensive cyber operations to contend with more advanced adversaries.

That said, most victims of Iranian cyber operations are in Iran or the large Iranian diaspora—the so-called internal enemies that Tehran's leadership fears. The early and effective adoption of the internet and social media by regime opponents and critics has fed the perception of Tehran's hardliners that foreign powers are conspiring to subvert the Islamic Republic through new technologies. But the targets of Tehran's digital surveillance include not only human rights defenders and perceived enemies of the state but also apolitical cultural institutions and even Iranian government agencies. Digital espionage and disruptive attacks against government critics have demonstrated to the Iranian public that its online activities are not outside the reach of the state.

This report provides a historical analysis of the activities and observed capabilities of Iranian threat actors who perform offensive cyber operations, most likely on behalf of the Islamic Republic. For purposes of maintaining a consistent terminology, the cyber activities covered in this report are framed in terms of "offensive cyber operations," which in the U.S. Department of Defense's words are actions "intended to project power by the application of force in or through cyberspace,"[1] or through distinguishing the intended effects (such as disruption, exfiltration, or destruction). This narrows the scope of research to intelligence and other offensive actions, rather than the full realm of Iranian government attempts to build influence online or control information.

Hackers working in coordination on cyber operations are described as "threat actors,"

although groups can have a single member and their composition can change over time. The terms "state-sponsored" or "state-aligned" are used throughout this report to reflect the direct relationship between the attackers and the Iranian government that is accounted for throughout the operations.[2]

Forensic artifacts and other records collected from cybersecurity research provide unprecedented insight into the security and intelligence priorities of the Iranian regime. The true intent of an attacker is not always evident in an intrusion. The compromise of a system for espionage or reconnaissance can later provide an electronic foothold used for sabotage. While Tehran has conducted highly visible attacks against rivals during times of conflict, the decade-long history of Iranian cyber operations reveals that the primary reason for such campaigns appears to be espionage.

Iran has been the target of espionage and destructive coercive measures launched by foreign states, including not only the United States and Israel but also Canada, France, Russia, and the UK. These attacks further motivated Tehran to develop indigenous defensive and offensive cyber capabilities as well as a credible retaliatory threat. These exchanges are directly correlated to Iran's domestic and geopolitical climate, which has been reflected in the reduction of disruptive attacks since the signing of the 2015 nuclear deal, formally known as the Joint Comprehensive Plan of Action (JCPOA).

While Tehran has conducted highly visible attacks against rivals during times of conflict, the decade-long history of Iranian cyber operations reveals that the primary reason for such campaigns appears to be espionage.

The primary source of data used in this report is documentation collected from attacks against a variety of nongovernmental organizations (NGOs) and other targets, both inside Iran and abroad. Forensic investigation techniques provide a broader perspective on the range of activities of threat actors, helping to identify specific participants and their potential connections to Iranian governmental entities. For example, the "sinkholing" of malware—the interception of communications through the redirection of domain names—provides insight into both the perpetrators and the victims of such campaigns. In other cases, the lack of professionalism by Iranian groups has led to the disclosure of names, aliases, and email addresses of their members in malware code and domain registration records.

This first-hand research complements numerous reports—based also on primary source material—published by cybersecurity companies on specific Iran-related incidents or threat actors. These publications provide alternative insights into Iran's targeting of other sectors outside the authors' immediate perspective, such as defense companies and gov-

ernments. An index of these reports will be made available online.[3] Interviews with targets of Iranian campaigns—including activists and scholars based in Iran and abroad—help elucidate Tehran's motivations and place the attacks in a broader context. Interviews with cybersecurity professionals similarly provide background on larger industry trends.

The intent of this report is to strengthen policy discussions of Iran's cyber operations by increasing public knowledge about the nature of such activities. Since cybersecurity research is typically limited to disclosures of specific threat actors or incidents, such publications do not provide insight into larger motivations and observable trends. This report differs in that it considers the historical patterns and the broader context of Iranian cyber operations, particularly their relationship to changing political conditions. It also emphasizes the overlap between Iranian campaigns conducted against foreign government institutions and/or corporate entities and those directed against human rights and civil society organizations, commonly neglected stakeholders in cybersecurity policy debates.

A better understanding of the history and strategic rationale of Iran's offensive cyber operations must inform U.S. strategy toward Iran and future U.S. responses to Iran's actions. This is especially true given the United States is reliant on an inadequately guarded cyberspace and should anticipate that future U.S. cyber attacks against Iranian targets could trigger retaliatory attacks on U.S. infrastructure. Iran's recent history suggests such an outcome.

CHAPTER ONE

IRAN: TARGET AND PERPETRATOR

Since the first publications on Iranian cyber activities in the summer of 2012—disclosing a malware agent named Madi—cybersecurity companies and Western government agencies have routinely documented intrusions, disruptions, and other malicious activities originating from Iran.[4] Yet aside from attacks that sought to subvert foreign infrastructure, these reports have rarely provided context about Tehran's offensive cyber operations and the motivations for attacks.

Tehran's perspective is shaped by the many attacks that have targeted its own infrastructure. Since Iran's covert nuclear facilities were exposed by an opposition group in 2002, numerous foreign actors have staged intrusion operations that sought to gain access to Iran's nuclear facilities, economic infrastructure, military apparatus, and governmental institutions, for both espionage and sabotage.[5]

Indeed, the most prominent example of modern cyberwarfare was the sustained campaign of sabotage—unprecedented in its sophistication and preparation—carried out by the United States and Israel against Iran's nuclear facilities. In what was known as Operation Olympic Games, the malware agent Stuxnet was used to sabotage components of the Natanz uranium enrichment facility, resulting in the destruction of over 1,000 centrifuges and setting back Iran's nuclear progress by more than a year. This marked one of the first known uses of offensive cyber operations as a coercive measure between states.[6]

While Stuxnet was solely intended to degrade Iran's nuclear program, other campaigns sought to sabotage the country's financial and oil infrastructure. In May 2012, a consor-

tium of researchers disclosed another destructive operation against Iran.[7] Malware agents known as Wiper and Flame, successors to Stuxnet, had been discovered when Iran's Ministry of Petroleum and the National Iranian Oil Company computers were disabled, their hard drives overwritten in a unilateral operation reportedly conducted by Israel.[8]

Coercive cyber operations targeting Iran continued following Operation Olympic Games. In June 2012, amid stalled nuclear negotiations between Iran and international powers, Tehran's minister of intelligence claimed the country's nuclear facilities were subject to another "massive cyber attack."[9] Later that year, Iran alleged additional disruptive operations targeting its Central Bank, Ministry of Culture, and drilling platforms operated by the Iranian Offshore Oil Company.[10]

In addition to sabotage, foreign intelligence agencies have continually targeted Iranian infrastructure for purposes of espionage, a fact made public to Iran through the intelligence disclosures of Edward Snowden. A former U.S. National Security Agency (NSA) worker, Snowden leaked a presentation on a tool known as Boundless Informant showing Iran to be one of the most highly surveilled countries in the world: billions of Iranian internet and telephone records have been collected by the intelligence agencies of the United States and its partners. In fact, Iran is so frequently surveilled that a Canadian espionage operation targeting Iran once stumbled across a French-run intelligence operation that had compromised the very same network.[11]

HOW IRAN EMBRACED CYBER REPRESSION

Iran's Supreme Leader Ayatollah Ali Khamenei has long believed Washington aspires to overthrow the Islamic Republic by instigating mass mobilization along the lines of the 1989 Velvet Revolution that toppled the Communist regime in Czechoslovakia.[12] Following similar logic, Iran's first cyber operations were motivated by fears that the internet facilitated external threats to regime stability. Tehran often labels the online dissent of its citizenry as cyberwarfare orchestrated by its enemies, namely the United States, to subvert the Islamic Republic. Western government support for unrestricted internet access and Persian-language satellite television stations—such as BBC Persian TV—are perceived as key elements of this strategy. The advent of social media sites, such as Facebook and Twitter, and messaging apps, such as Telegram, are especially threatening given they challenge the Iranian government's long-standing monopoly over media and communications.

Khamenei's greatest concerns were realized when the June 2009 contested reelection of hardline president Mahmoud Ahmadinejad—amid widespread allegations of fraud—provoked Iran's largest popular uprisings since the country's 1979 revolution. It was also a

pivotal moment in the Iranian government's embrace of offensive cyber capabilities, as this mass mobilization—known as the Green Movement—became one of the first known targets of the regime's operations. The online contest between the opposition, using the internet to coordinate political resistance, and the government, attempting to repress mobilization, set the stage for future conflicts, including those with foreign powers.

Soon after an estimated 2 million Iranians protested in Tehran on June 15, 2009, supporters of the Green Movement began to battle the government over control of information.[13] When the authorities expelled foreign media, interfered with mobile phone networks, and arrested prominent critics, the internet became a primary channel for coordination amid the chaos. In response, the U.S. Congress, then U.S. president Barack Obama's administration, and American technology companies sought to maintain Iranian users' access.[14]

An Iranian hacker breached the Dutch security company DigiNotar to fraudulently issue encryption certificates that allowed Tehran to spy on all domestic Gmail users, one of the largest security breaches in the history of the internet.

During the Green Movement, pro-regime hackers engaged in a multipronged strategy of intrusions, disruption of websites, and network surveillance. Between December 2009 and June 2013, a group calling itself the Iranian Cyber Army defaced websites associated with Iran's political opposition, Israeli businesses, independent Persian-language media, and social media platforms, posting pro-government messages. When human rights activists and opposition leaders called for street protests, critical websites were subject to a deluge of malicious internet traffic to disrupt access, known as distributed denial-of-service (DDoS) attacks.[15] Government critics were spied on with malware posing as information on upcoming protest plans and public scandals.[16] An Iranian hacker breached the Dutch security company DigiNotar to fraudulently issue encryption certificates that allowed Tehran to spy on all domestic Gmail users, one of the largest security breaches in the history of the internet.[17]

Ultimately, the brutality, surveillance, and censorship exercised by the security forces debilitated the Green Movement, and by 2011 public protests had subsided. Security agencies had adapted to the modern digital environment, with interrogations by the IRGC including an intimate review of an arrestee's personal life based on printed copies of his or her online communications and social media. An IRGC chief later said that suppressing the demonstrations required widespread arrests, massive repression, and cutting off means of mass communication, such as cellphones and the internet.[18] The Green

Movement demonstrated to the Islamic Republic that the internet could be used as an instrument of mass mobilization and posed an effective challenge to the regime's long-held information monopoly.

The tactics, tools, and threat actors that arose during this domestic challenge to regime stability would foreshadow the cyber posture of Iran toward a wider set of internal and foreign threats. A recurrent theme since the outset of Iran's cyber operations is that Iranian campaigns do not maintain clear boundaries between operations directed against its internal opposition and those directed against foreign adversaries.[19] The same infrastructure and tools used by Iranian threat actors for campaigns against the American defense industry are also used to target Persian-language women's development programs; the same malware used in destructive attacks against Saudi government institutions had been previously used for surveillance against members of the Green Movement opposition.

IRAN'S OFFENSIVE CYBER CAPABILITIES

Cyber operations have provided Tehran less risky opportunities to gather information and retaliate against perceived enemies at home and abroad. Before information communication technologies were widely available, the Iranian government's foreign intelligence operations centered chiefly on recruiting agents to spy on and assassinate political dissidents or the diplomats of rivals. These operations usually resulted in international embarrassment when the attackers were caught and condemnation when they succeeded. Compared to clandestine in-country operations, offensive cyber capabilities provide stronger deniability and have thus far been less likely to lead to retaliation upon discovery.

Over the past decade, offensive cyber operations have become a core tool of Iranian statecraft, for the purposes of espionage, signaling, and coercion.

Over the past decade, offensive cyber operations have become a core tool of Iranian statecraft, for the purposes of espionage, signaling, and coercion. Accounts of Iran's offensive cyber operations follow a consistent pattern across campaigns and among different threat actors. Operations focus on well-defined sets of targets and are less sophisticated than the campaigns of state-sponsored threat actors in other countries—to credibly signal threats and create deterrence requires assured repeatability, a capability that Tehran generally still lacks.

Moreover, the level of professionalization, preparation, and investment necessary to conduct an operation like Operation Olympic Games remains far outside the capacity of

Iranian threat actors. Unlike the cyber operations of the United States and Israel, which are conducted by professional intelligence services supported by billion dollar budgets, Iran's offensive and defensive capabilities are disorganized and modestly funded.[20] Thus, while Iran frequently turns to disruptive attacks to apply pressure, it faces a ceiling of capability and opportunity in its ability to threaten opponents. Tehran's clandestine human intelligence gathering in foreign countries, particularly outside the Middle East, is of similarly low sophistication.

Tehran rarely claims responsibility for offensive cyber operations attributed to it, including those espousing support for the Islamic Republic, and has made contradictory statements on its cyber posture. Iranian authorities have a history of embellishing the country's military capacity, including for cyber operations. In responding to a series of disruptions of its own infrastructure in October 2012, then minister of intelligence Heidar Moslehi asserted that "the Islamic Republic is so powerful in the cyber space that [even] leaders of the arrogant powers admit and acknowledge our country's successes."[21] However, IRGC commander Mohsen Kazemeini also claimed that the IRGC's cyber-warfare division was not tasked with conducting offensive operations.[22] Official rhetoric also appears to conflate the state's effort to push online propaganda with offensive cyber capabilities, leading to claims of tens of thousands of cyber warriors.

Iran has used reports of destructive incidents to portray itself as a victim of foreign aggression, deflect attention away from its own actions, and boast of its ability to neutralize potential attacks. When accused by the United States of having conducted a disruptive attack against American banks, Iran's Deputy Foreign Minister Hossein Jaberi Ansar responded that "the U.S. government, which put millions of innocent people at the risk of an environmental disaster through cyber attacks against Iran's peaceful nuclear facilities, is not in a position to level accusations against the citizens of other countries, including those of Iran, without substantiated evidence."[23] Iranian officials appealed to international institutions for relief after the country had been affected by the malware agents Flame and Wiper, a move that aligned with its calls for greater United Nations (UN) control over the internet.[24]

In public statements, Iran has often emphasized its defensive capabilities, announcing in 2015 that its Cyber Attacks Emergency Center had successfully managed to thwart U.S. cyber attacks against the country's industrial infrastructure.[25] Iranian military officials regularly announce new defense products developed by domestic contractors, the most prominent example being the antivirus software Padvish.[26] Despite these claims, Iran has shown little success in fostering a mature cybersecurity industry and lags behind both developed economies and key regional rivals in terms of investing in defense or formulating national policies to secure critical infrastructure.

While the Iranian government has committed tens of millions of dollars to cybersecurity in recent years, the scale of these investments pales in comparison to the billions spent annually by the U.S. government or the hundreds of millions spent individually by American banks.[27] Were Iran to focus on improving its defensive capabilities, it would still face significant constraints related to sanctions, bureaucratic inefficiency, and a deficit of specialized expertise. Given the sophistication shown by its adversaries, assertions about the quick detection and remediation of foreign intrusions into Iranian networks should be viewed skeptically, a defensive posture that is unlikely to change.

Iran is generally perceived as a third-tier cyber power, lacking an advanced indigenous cybersecurity apparatus capable of carrying out sophisticated operations like China, Israel, Russia, and the United States.

Despite its confident claims, Iran is generally perceived as a third-tier cyber power, lacking an advanced indigenous cybersecurity apparatus capable of carrying out sophisticated operations like China, Israel, Russia, and the United States.[28] While technical sophistication does not impede Iranians from conducting successful cyber operations, those actions reflect a disorganization and lack of professionalism that runs contrary to what would be expected of a state actor and limits their capabilities. Tehran's political and economic isolation has further constrained it from acquiring technology and expertise from foreign governments or companies, and little evidence exists that would indicate substantial cooperation with other nations in the development of its offensive cyber capabilities.

THE DIFFERENCE BETWEEN ESPIONAGE AND SABOTAGE

Media accounts of cyber operations often paint incidents with a broad brush, labeling all intrusions as attacks regardless of whether the outcome was destructive.[29] Offensive cyber operations, however, can be more accurately labeled according to their intent and impact, distinguishing espionage and sabotage. Iranian actors have both engaged in intrusions to extract information from foreign networks (espionage, information gathering) and performed destructive actions to punish or coerce adversaries (sabotage), with a gray area in the middle related to signaling and other motivations. Understanding this difference is important in assessing Tehran's strategy and the legality of its operations.

International law differentiates activities that are legal, though not desirable, from those that are illegal and could prompt dangerous escalation.[30] Just as international law differ-

entiates traditional espionage from coercion or violence, these same principles also apply to cyber espionage. Legal scholars have asserted that "mere intrusion into another State's systems does not violate the non-intervention principle."[31]

Indeed, given the growing number of nations with offensive cyber capabilities, espionage and information gathering through cyber operations has increasingly become accepted as an international norm.[32] While the United States naturally denounces Tehran's targeting of State Department employees, for example, such incidents mirror similar espionage operations against Iranian diplomats by U.S. and other Western intelligence agencies.[33]

International law experts have provided frameworks for determining what constitutes an "armed attack" in cyberspace, based on severity, invasiveness, directness, and other factors. Such frameworks also reinforce the importance of terminology, differentiating, for example, espionage against the Navy Marine Corps Intranet from a destructive incident such as Iran's attack on Saudi Arabia's and the world's largest oil company, Saudi Aramco.[34] Relatedly, scholars have noted that Iran's use of proxies in offensive cyber operations does not absolve the government of legal obligations or repercussions for their outcome, based in part on international case law from the 1979 Iranian hostage crisis.[35]

Consistent evaluation of the legality of Iranian cyber operations provides clearer public benchmarks for assessing when Iran violates internationally respected principles and engages in illegitimate behavior. As Tehran continues to conduct offensive cyber operations, it is important for policymakers to assess the intent, scope, and legality of Iran's actions before considering counter responses.

CHAPTER TWO

IRAN'S CYBER ECOSYSTEM: WHO ARE THE THREAT ACTORS?

The Islamic Republic of Iran is unique in that its most powerful officials—namely Supreme Leader Khamenei and the Islamic Revolutionary Guard Corps—are inaccessible, while its most accessible officials—including Foreign Minister Javad Zarif—are far less powerful. Iran's offensive cyber activities are almost exclusively overseen by the IRGC—likely without the oversight of the country's publicly "elected" officials—and composed of a scattered set of independent contractors who mix security work, criminal fraud, and more banal software development. While the relationships between proxies and governments can range from passive support to complete control, Iran's indigenous threat actors maintain an arm's-length relationship to the state, with certain operations orchestrated to meet the needs of the government.[36]

After successfully suppressing the 2009 Green Movement and first detecting the Stuxnet attack in 2010, Iranian threat actors conducted sustained campaigns against domestic and foreign adversaries. These indigenous operations appear to be performed by small groups of individuals that have varying levels of technology experience with no more than ten people per team. These campaigns and the resources produced by the groups range from rudimentary to relatively professional, but most actors still face a low capacity ceiling.[37]

Though U.S. officials and some cybersecurity companies have speculated that Tehran has received technical assistance from countries like Russia and North Korea, the level of sophistication is commensurate with the established practices of amateur hacking communities inside Iran.[38] While Iranians have demonstrated talents in social engineering and

embedding themselves in compromised networks, this alone is not indicative of external training or technological transfers.

On several occasions, Iranian threat actors have used off-the-shelf or pirated versions of professional penetration testing tools to conduct campaigns, but there is little indication of Tehran acquiring exploits or malware from foreign governments. Iran *has* acquired hardware for internet surveillance from Chinese telecommunication firms and maintains cooperative agreements with Russia on cybersecurity; however, these relationships differ from providing Tehran with offensive cyber capabilities.[39] No publicly documented or privately observed attack has demonstrated the use of tools or resources that are beyond the capacity of Iranian threat actors.

In principle, the tools and tactics used in cyber operations are subject to an exposure risk. Unlike conventional weapons, malware attacks or other cyber activities lose their effectiveness when discovered and when their functionality and infrastructure is documented. Describing a missile does not provide effective countermeasures, but describing malware can provide antivirus companies and system administrators the ability to protect systems. State-aligned threat actors will likely not employ the most sophisticated tools and strategies available to them unless the target is well protected and worth potentially exposing tradecraft to compromise. However, unlike in other countries, there are not observed examples from Iranian threat actors of escalation into more sophisticated attacks against hardened targets.[40]

Iranian threat actors conduct campaigns with established toolkits that sometimes last for years and ensnare hundreds of targets. However, the fluid nature and decentralization of these groups make them relatively difficult to track. Malware that is publicly attributed to Tehran is often abandoned immediately on exposure, and identifiable members appear to change groups over time. Some groups seem to split up, have members move elsewhere, or even collaborate, further blurring lines.[41] For example, while an IRGC-affiliated group labeled Rocket Kitten was the most active operator for a two-year period (2014–2016), attracting press attention as Iran's premiere threat, it has since faded into quiescence, eclipsed by the actor Oilrig.[42]

Despite their substantial financial impact, Tehran's disruptive operations against foreign targets have been technically simple. The compromise of a small number of IT personnel enabled the destruction of data on computers maintained by Saudi Aramco, eventually resulting in hundreds of millions of dollars in damage.[43] In only a few campaigns have Iranian threat actors shown the professionalism and sophistication approaching that expected of a nation-state actor; in one such case, the operation could be tied directly to the Ministry of Intelligence (Magic Kitten, discussed later).[44]

Success can often be attributed to security failures and to poor protection of infrastructure on the part of the victim, alongside opportunistic targeting and patience by the attacker. The defacement of Voice of America's websites by the Iranian Cyber Army, one of the first disruptive attacks by Iran against the United States, was accomplished through social engineering the news agency's domain name service provider.[45] Other basic security failures gave Iranians a toehold in the networks of Las Vegas Sands Corp. after its owner, Sheldon Adelson, advocated military force against Iran.[46] Symantec, an American cybersecurity company, noted that the perpetrators of a recent Saudi-focused campaign had invested a "significant amount of preparatory work for the operation," but the custom malware was described by Russian cybersecurity firm Kaspersky as "generally of low quality" partially derived from open-source toolkits.[47]

Similarly, a major attack on the American financial sector—known as Operation Ababil—which caused hundreds of millions of dollars in damage, was described as one of the largest DDoS attacks known at the time. Yet it took only a few young Iranian computer experts, breaching thousands of websites that were running vulnerable software, to pool enough bandwidth to overwhelm the infrastructure of banks and cause unpredicted software failures.[48] Thus, while Iranian threat actors have limited capacity, through basic tradecraft and persistence they can still be effective at espionage and sabotage.

The overall sophistication and dedication observed in such campaigns has not significantly changed in the decade that Iran has engaged in offensive cyber operations—the attacks documented against Las Vegas Sands Corp. in 2014 are comparable to those used against Saudi Arabia in renewed hostilities over the course of 2016-2017. Indeed, many research disclosures cover groups that have been active for several years, using the same malware with only incremental changes over the course of time.

While sophistication alone can be a superficial metric of posed threat, Iranian operations do not demonstrate the common technical precautions taken by other nation-state actors (such as obfuscating malware), and, even with strong social engineering capabilities, attacks are often betrayed by a lack of investment in nontechnical resources (such as fluency in English or personal tailoring of messages).[49] These resource constraints also account for why Iranians are more effective at compromising dissidents—Iranian threat actors understand their target's context and language, as opposed to when they are tasked with European languages or other cultures. Iran shows little indication of becoming a first-tier cyber power in the foreseeable future unless it begins to further organize its operations and invest in professionalism.

MAGIC KITTEN

In January 2015, the German news outlet *Der Spiegel* released previously unpublished documents on cyber espionage conducted by American intelligence agencies.[50] One of them revealed an NSA tactic labeled "fourth party collection," which is the practice of breaking into the command and control infrastructure of foreign-state-sponsored hackers to look over their shoulders. The presentation describes a real-life example of acquiring intelligence and stealing victims from a group code-named VOYEUR by the NSA, otherwise known as Magic Kitten.

Magic Kitten appears to be among the oldest and most elaborate threat actors originating in Iran. It is also distinct from other groups because of its apparent relationship with the Iranian Ministry of Intelligence rather than the IRGC. However, Magic Kitten's activities mirror those of other groups, with the primary targets being Iranians inside Iran and Tehran's regional rivals. The earliest observed samples of Magic Kitten's custom malware agent dates to 2007, well before other known malware apparently originated, and the threat actor continues to be active.

Magic Kitten appears to exercise the most mature tradecraft of Iran-based threat actors. It has opportunistically compromised dozens of websites at random (including those of an Indian hospital, an Italian architect, and a well-known Canadian comedian) to create a relay network to hide its operations. Such attention to tradecraft appears elsewhere in Magic Kitten's operations, including in the design of malware, which is modular in nature.

Magic Kitten has not been observed using sophisticated exploits and instead appears to rely on social engineering and other common tactics to deceive users. In the case of the journalist Vahid Pour Ostad, the malware was sent by his former Ministry of Intelligence interrogator with a threat attached and relied on private records that would have been available only to government actors. This coordination represents both independent confirmation of the NSA's attribution and an extreme example of the strategies employed by Magic Kitten. Other samples of the malware agent appear to have been delivered posing as Turkish asylum forums for Syrian refugees.

The NSA presentation also provides a window on Magic Kitten's targets up to May 2011, portraying an operation focused on North America, Europe, and the Middle East. These campaigns continued through the June 2013 presidential election of Hassan Rouhani, provoking a blogpost from Google about related attacks.[51] As the election approached, exposed logs showed the daily capture of dozens of accounts connected to Iranian cultural and media figures, graduate students, and social activists (including individuals that would later join the Rouhani administration). Magic Kitten continued to target Iranians after the election, attempting to unmask pseudonymous internet users by baiting them with content on women's rights and the security establishment.

Like other Iranian operations, Magic Kitten maintains a strong secondary interest in conducting espionage against regional targets and international foreign policy institutions. CrowdStrike, another American cybersecurity company, accounts for part of this focus on "international corporations, mainly in the technology sector" and other political targets.[52] An NSA slide with a victim map portrays a broad-reaching operation targeting nearly every country in the Middle East. Sinkhole data collected from expired domains previously used as relays and other fallback infrastructure suggest that Magic Kitten, or the malware agent used, continues to actively compromise individuals in Germany, Indonesia, Iraq, Lebanon, the Netherlands, Palestine, Pakistan, Qatar, Sweden, Switzerland, Thailand, and the United Arab Emirates. Notably, compromised individuals in Iraq were also typically in Iraqi Kurdistan, mirroring a common pattern with other threat actors.

A diagram within the NSA presentation suggests that the malware agent employed by Magic Kitten was also used at the time by Iran's Shia Lebanese proxy Hezbollah, under independent infrastructure. While Hezbollah has been known to maintain its own offensive cyber operations and engage in intelligence sharing with Iran, there has been little prior evidence of direct sharing of tools.[53]

UNDERSTANDING IRANIAN GOVERNMENT INVOLVEMENT AND ATTRIBUTION

It is often difficult to determine the origins and perpetrators of Iranian offensive cyber operations, as these campaigns may disappear as quickly as they appear. Public exposure often leads them to change tactics and abandon tools, making tracking even more difficult. The history of cyber operations targeting Iranians and originating from Iran is populated by groups that arise out of nowhere and conduct campaigns for ambiguous reasons over a finite time span, then disappear. This unusually frenetic character conspicuously differentiates the Iranian hacking ecosystem from that found elsewhere, particularly those tied to state actors in advanced countries.

The history of cyber operations targeting Iranians and originating from Iran is populated by groups that arise out of nowhere and conduct campaigns for ambiguous reasons over a finite time span, then disappear.

The amateur hackers connected to the Iranian defacement community have long been politically engaged and have often vandalized foreign sites for ostensibly nationalistic reasons.[54] In one of the first international incidents attributed to Iran, domestic hacking groups in mid-2008 exchanged tit-for-tat defacements with competitors in neighboring Arab countries after the official sites of Grand Ayatollah Ali al-Sistani were vandalized with anti-Shia content by an Emirati hacker. Such defacement activities can often evolve into state-affiliated activities: one of the participants in the anti-Sunni website-defacement campaign in 2008 was later linked to the Iranian Cyber Army. This transition from patriotic hackers to state-aligned threat actors, and the ambiguity between civic nationalism and state involvement, mirrors the apparent development of cyber communities in China and elsewhere.[55]

In only two incidents have Iranian government entities taken direct credit for the defacement of political opposition sites, both attributed to branches of the Revolutionary Guard. The first case was the March 2010 takedown of sites connected to the organization Human Rights Activists in Iran, which was alleged to be training cadres to mobilize against the regime like the Velvet Revolution. The attack relied on the arrest of a website administrator inside the country rather than on complicated tactics. The arrests and destruction of data had a lasting impact on the organization by instilling fear in members and giving rise to rumors about collaboration with the government.

The second government-initiated campaign, carried out during a Shia holiday in December 2013, led to the defacement of nine human rights and independent media websites

with a Quranic verse in Arabic and Persian. The IRGC's Public Relations Department announced that the operation had been conducted by the Revolutionary Guard's Kerman Branch and claimed that the defaced websites had been established by the country's enemies and supported by internal seditionists.

In most cases, Iran uses cutout or proxy organizations, allowing it to keep some distance from the disruptive incidents and propagandistic defacements. These cutouts represent themselves as patriotic Iranians or pan-Islamic movements acting independently in defense of the supreme leader, national sovereignty, and religious ideals. Conducting offensive cyber operations through covert organizations provides Tehran plausible deniability for any attacks, thereby protecting its claim to victimhood while also allowing the state to signal its intentions to its opponents. These tactics are effective: there is still no definitive public agreement on who was behind the Yemen Cyber Army's attacks that led to stolen Saudi Arabian Ministry of Foreign Affairs documents being published by WikiLeaks, with the consensus split between Iran and Russia.[56] The cutouts tend to develop their own mythology and continue to be treated as active threats past their expiration date, bolstering perceptions of Iran's capability.

Conducting offensive cyber operations through covert organizations provides Tehran plausible deniability for any attacks, thereby protecting its claim to victimhood while also allowing the state to signal its intentions to its opponents.

Nevertheless, a comprehensive study of Iran-linked cyber operations often reveals Tehran's hand in such proxies. When the U.S. Justice Department unsealed its Operation Ababil indictment in March 2016, it named two Iranian corporate entities that employed at least seven individuals who had been contracted by the Iranian government.[57] The indictment implicated three of the participants as being part of the Sun Army, an Iranian cutout defacement group. The Sun Army followed the typical pattern found with the Iranian Cyber Army and other state-aligned defacements, arising out of nowhere to perform targeted political acts over a short life span. Its first documented defacements, in February 2010, were of sites connected to now-detained opposition leader Mehdi Karroubi. The vandalism accused him of being a traitor and was timed to blunt planned antigovernment street protests.[58]

As Iran's cybersecurity landscape has professionalized, some defacement groups have sought to convert their infamy into corporate success. Based on the disclosure of personal information about threat actors, there are indications that those engaged in Iranian offensive cyber operations work within corporate entities (such as IT consultancies) or contractors of Iranian security forces.[59] For example, aspects of the Madi espionage campaign

implicated the Mortal Kombat Underground Security Team, a small Iranian group that has attempted to sell spyware and other hacking tools since at least 2008.[60] The frequent overlap of legitimate digital commerce sites and servers used for intrusion campaigns is demonstrative of these blurred lines—a company might simultaneously provide web design services for businesses and hack for the government.[61]

The transition of amateur hackers into contractors for state security agencies is reflected in basic qualities and patterns of life found across most threat actors. There are clear indications that the threat actors documented are solely Iranians operating inside Iran, not diaspora Iranians or non-Iranians. At the most basic level, they tend to follow the normal patterns of life of office workers, being active during the Iranian workweek (Saturday through Wednesday) and dormant during Iranian holidays, particularly the long holiday of Nowruz, the Persian New Year.

Iranian threat actors have often used pornography as bait in their spearphishing campaigns and display an irreverent sense of humor.

Disclosures of aliases and real names, which may be discoverable because of a disregard for operational security due to insulation from repercussions or a lack of professionalism, help reveal both the lives and the motivations of Iranian threat actors. While those behind the groups may be nationalists or ideologically aligned with the regime, they do not appear to be enrolled members of the military or security apparatus. These individuals and groups also differ in social and religious predilections; some participants promote the use of narcotics and trade pornography on personal social media, while others are devoutly religious and embed Islamic references in malware code. Iranian threat actors have often used pornography as bait in their spearphishing campaigns and display an irreverent sense of humor.

CRITERIA FOR INDEPENDENT ASSESSMENT OF STATE INVOLVEMENT

Campaigns conducted against dissidents and others inside Iran provide the most direct evidence of government involvement. Whereas it can be difficult to trace the consequences of foreign espionage, for those on the ground the implications are more direct and tangible.[62] As a pattern builds between cyber operations and the offline actions of security forces, the relationship between both becomes clearer.[63] While these cases of collaboration are discernible in only a few threat actors, the patterns support a broader narrative around the intrusion ecosystem.[64] Indications that Iranians undertaking offensive cyber operations are associated with the government include the following:

- The campaigns have been conducted based on information that appears to have been provided by security agencies. In certain cases, the campaigns have been carried out in coordination with government employees and in advance of the arrest of the target.
- The targets of such operations align with the sensitivities of the Islamic Republic, and certain individuals are targeted repeatedly by multiple threat actors over time.
- Persistent and costly campaigns have been sustained against thousands of targets without an apparent financial motive and without clear indication of the end use of the data obtained by intrusion.

In rare cases, potential ties to the government are even disclosed by the participants themselves. A malware developer associated with the Rocket Kitten group, Yaser Balaghi, was identified by name based on a pseudonym found in the malware's code. In a résumé from 2013, Balaghi listed past information security projects and a history of conducting hacking projects under contract to an otherwise unnamed "cyber-organization."[65] Balaghi is not alone in listing his hacking activities on his résumé; still other pseudonyms embedded in malware code used against Saudi Arabia and internal dissidents can be associated with LinkedIn profiles describing their experience as an "Information Security Researcher" with a "Secret" group.

To add a complication common in cybersecurity research, it is often difficult to distinguish commonplace electronic fraud from politically motivated disruptions and state-sponsored surveillance efforts, especially where the attacks are not sophisticated. In at least one case, Iranians that had staged persistent attempts against U.S. foreign policy organizations and two European foreign ministries had also maintained infrastructure linked with commercial banking fraud.[66] In another example, the same social engineering skills used by an individual behind the Iranian Cyber Army defacements also proved successful in a career in the commercial theft of domains and PayPal fraud. More recently, in an indictment against an Iranian accused of attempting to extort HBO with stolen copies of unreleased television episodes in the summer of 2017, the U.S. Department of Justice claimed that the same individual had worked on behalf of the Iranian government to target military systems and Israeli infrastructure.[67]

Analyses of Iranian offensive cyber operations often rest on the country's strict domestic controls as an indication of endorsement—that the government would not allow something to happen that it didn't want to occur. However, Tehran's controls are not so absolute, and many of the operations could occur surreptitiously given their simplicity. Cyber activity emanating from Iran could theoretically be conducted without the state's sanction, consent, or even knowledge. Daily, millions of Iranians circumvent censorship using antifiltering tools that allow them to bypass network restrictions and encrypt their

communications against surveillance. These tools provide space for Iranians to engage in actions against the government without persecution, and similarly can conceal cyber activities. Therefore, an Iranian origin does not alone indicate state sponsorship.

Nor does the financial damage resulting from an operation, the political implications of the campaign, or the number of targets necessarily directly correlate with the probability of government involvement. The destructive operations conducted against Saudi Aramco resulted in millions of dollars in damages, yet the malware was unsophisticated and the attack did not require significant resources, putting the incident plausibly within reach of a sole individual acting without sponsorship. Such straightforward metrics of harm, then, are poorly informative of the degree of governmental involvement in cyber activities originating from Iran.

GOVERNMENT ENTITIES AND THREAT ACTORS

The coordinated timing of cyber operations with politically motivated arrests are a strong indication of the Iranian government's direct involvement. Since at least July 2014 a pattern has emerged: individuals in the custody of the IRGC are forced to provide access to their online accounts and devices, which are then immediately used to conduct spearphishing attacks associated with known threat actors.

A vivid example of this coordination is the case of Iranian-American Siamak Namazi, a forty-six-year-old Dubai-based energy consultant and previously a scholar at the Woodrow Wilson International Center for Scholars in Washington, DC. In October 2015, he was arrested by Iranian security forces months after having had his passport confiscated while visiting the country. Within hours of his arrest, Namazi's Google and Facebook accounts initiated conversations with his wide array of foreign policy and media contacts. The intruder, pretending to be Namazi, sent contacts an article about the recent nuclear deal and in poor English solicited edits on the document. This message was accompanied by an email directing the target to a fake Google site requiring visitors sign in to their account to view the document, a credential theft attempt connected to Rocket Kitten. Numerous individuals were compromised in this campaign, including scholars, U.S. State Department employees, and one prominent journalist whose Gmail account—which included communications with former U.S. secretaries of state, CIA directors, and other foreign ministers—was overtaken by the Iranian hackers for nearly two days.[68] This pattern has been repeated in numerous cases involving other Iranians, dual nationals, and foreign nationals detained in Iran.

Cyber operations have also been documented in preparation for arrests.[69] A prominent example of target selection prior to arrest is the case of Babak Zanjani, an Iranian-Danish businessman who had been personally sanctioned by the United States and European Union for involvement in Iranian sanctions evasion. After months of claims regarding his role in the embezzlement of oil revenue, a process that included a parliamentary investigation, at the end of December 2013 Zanjani was arrested and subsequently charged with "corruption on earth."[70] After an opaque judicial process, in March 2016 he was condemned to death, a sentence the Ministry of Justice indicated could be commuted if Zanjani cooperated in recovering Iran's foreign assets.

This overarching trend points to probable relationships between certain threat actors and the intelligence agencies, a business relationship that has been revealed when Iranians have been indicted by the United States for hacking.

A persistent effort targeted Zanjani's personal accounts and business infrastructure in the weeks immediately preceding his arrest. Iranian threat actors sought access to Zanjani's iCloud services and successfully compromised employees associated with his holding company, the Sorinet Group.[71] These activities indicate that in advance of the arrest of Zanjani, the group (Flying Kitten) had acquired access to the confidential information of Sorinet subsidiaries and personnel; however, it is not clear whether any material accessed during this time was used in the investigation or prosecution of Zanjani. The case of Zanjani reflects a broader trend witnessed with other cases; Iranian threat actors frequently pursue online the types of individuals commonly persecuted by the Islamic Republic offline.

The association between Iranian-origin cyber activities and Iran's intelligence agencies is further supported by the fact that the data acquired during such operations is rarely disclosed. The Navy Marine Corps Intranet breach, the Las Vegas Sands Corp. incident, and the compromise of State Department employees have all led to the exfiltration of substantial amounts of highly sensitive information. There is no indication of ulterior motives, such as fraud, extortion, humiliation, or disclosure to the hardline press.[72] The operations required costly infrastructure, including dedicated servers and dozens of domain names, in addition to personnel time. The activities must have provided some degree of income to their members, with the primary value being espionage. This overarching trend points to probable relationships between certain threat actors and the intelligence agencies, a business relationship that has been revealed when Iranians have been indicted by the United States for hacking.

CHAPTER THREE

IRAN'S EXTERNAL TARGETS

Given Iran's inability to effectively challenge or deter better-prepared opponents, it has employed opportunistic destructive attacks to demonstrate its ability to retaliate. Particularly in the Middle East, Tehran can implicitly threaten cyber operations against the poorly defended economic and infrastructure resources of its opponents in the event of hostilities. Indeed, the disclosure of targets and victims of Iran's regional cyber operations often include industries that appear to serve no other purpose than creating beachheads in rival countries, such as banks and airports.

The intended effects of disruptive operations can vary, ranging from intimidation to destruction for foreign targets, and from embarrassment to existential harm for domestic opponents. The targeting or compromise of systems can alone be sufficient to communicate Tehran's willingness and capability to inflict damage on opponents. This echoes Iran's occasional threat to close the Strait of Hormuz—through which nearly 60 percent of the world's oil supply passes on any given day—during times of crisis. Given the opacity of the Iranian government, however, the intended messages and expectations being signaled from Tehran can be easily misinterpreted, risking unintended conflict or escalation.

Such destructive attacks are rare, however, compared to Iran's espionage campaigns against foreign governmental and economic institutions. Increasingly these campaigns form not only the basis of retaliation during conflict but also an essential crisis response mechanism for handling emerging threats. For example, days after a September 2015 stampede killed over 450 Iranians attending the Hajj pilgrimage, domain names impersonating the Saudi government and Hajj Ministry were registered by known Iranian

threat actors.[73] As relations and communications rapidly deteriorated between the two countries, particularly over the fate of a missing diplomat, cyber espionage became an information gathering tool for Tehran.

Saudi Arabia aside, Denmark, Germany, Israel, and the United States are among the countries that have publicly disclosed espionage attempts by Iranian groups against their government, military, or scientific institutions.[74] Tehran also targets neighboring countries throughout the Middle East. Despite the various threat actors that operate on behalf of the Iranian government, their behavior patterns—including whom they target—are generally consistent over time.

THE UNITED STATES AND EUROPE

In September 2012, a group calling itself the Izz ad-Din al-Qassam Cyber Fighters announced it had begun a campaign of DDoS attacks against the U.S. financial sector. Prior to the campaign, the culprits had exploited vulnerabilities in the software of thousands of websites in order to create an attack platform under their control. With this army of servers located within well-connected hosting companies, the attackers could deluge their targets with high volumes of malicious traffic. In the first phases of Operation Ababil, the group targeted the U.S. banking infrastructure. Unprepared for such a volume of traffic (the U.S. Federal Bureau of Investigation stated the highest rate observed approached 140 gigabits per second, three times the capacity of the banks at the time), the victims' databases and systems crashed from the dramatic increase in requests.

An NSA briefing document also made clear the motivation for Operation Ababil: "[Signals intelligence] indicates that these attacks are in retaliation to Western activities against Iran's nuclear sector and that senior officials in the Iranian government are aware of these attacks."

Subsequent phases of the campaign were less effective as the financial sector steadily improved its defenses. By the fourth attempted attack, in July 2013, little visible impact resulted. Still, by the FBI's account, Operation Ababil locked hundreds of thousands of banking customers out of accounts for long periods of time and resulted in tens of millions of dollars in costs to remediate. An NSA briefing document also made clear the motivation for Operation Ababil: "[Signals intelligence] indicates that these attacks are in retaliation to Western activities against Iran's nuclear sector and that senior officials in the Iranian government are aware of these attacks."[75]

Operation Ababil remains the most destructive Iranian attack on the United States. While the International Atomic Energy Agency (IAEA) alleged that Tehran had electronically surveilled and tampered with the devices of visiting nuclear inspectors in 2011, little had been known about Iranian cyber espionage prior to 2012.[76] That summer provided the first public indication that Iranian threat actors had staged campaigns to spy on rivals.[77] The Madi malware campaign was reported to have compromised up to 800 victims over the course of a year. The countries and entities targeted were a harbinger of future Iranian cyber operations, including oil companies, U.S. think tanks, government agencies, engineering firms, financial institutions, and academia.

Iranians attempted to compromise the personal email accounts of members of the American team during the nuclear negotiations.

Several Western countries have provided evidence of Iranian cyber operations in indictments and security reports. In addition to Operation Ababil, Iranians were alleged to have gained access to the unclassified Navy Marine Corps Intranet, a system used to store unclassified information and communications, for several months starting in August 2013.[78] In the 2016 edition of an annual Ministry of Interior security assessment, the German government cited Iran as a new source of cyber espionage against the country, a disclosure that aligned with reports that the Bundestag had been affected by a malware operation that targeted visitors of the Israeli newspaper *Jerusalem Post*.[79]

Overall, however, cases of successful Iranian intrusions into American and European governmental infrastructure are rare, particularly highly secured, classified networks. Government agencies are typically hardened beyond the capability of Iranian threat actors to penetrate them. Consequently, Iranians have sought softer U.S. targets, launching spearphishing attempts on the personal email and social media accounts of U.S. government employees. While personal accounts are less likely to contain classified government information, they are also less likely to be properly secured, and often contain useful information such as private material and traces of professional communications.

For example, Iranians attempted to compromise the personal email accounts of members of the American team during the nuclear negotiations.[80] Similarly, after the 2016 U.S. presidential election, Iranian threat actors focused on former Obama staff, Republican members of Congress, supporters of Donald Trump's campaign, conservative media organizations, and nominees for political appointments in an apparent attempt to acquire intelligence on the new administration.[81] More recently these spearphishing campaigns have targeted critics of Iran in the U.S. Congress while new sanctions have been under consideration.

Tehran tends to target the foreign government personnel and agencies that focus on Iran, namely those in the United States or Europe who work on Iran policy or within Persian-language media, including Voice of America television and Radio Farda. Iranian threat actors have used the compromised accounts of prominent Iranian-Americans, international businessmen, and other dual nationals arrested by the IRGC to impersonate them and target the private email accounts of U.S. State Department personnel connected to Iran policy.

In contrast to the release of private emails by WikiLeaks during the 2016 U.S. election, which leveraged stolen emails for information warfare, Tehran's compromise of State Department employees' emails did not lead to visible sabotage or the disclosure of embarrassing material. While there have been dozens of attempts to target a wide array of American politicians and government employees, these intrusions were mostly opportunistic attempts that did not appear to escalate into more sophisticated operations.

Following the 2015 nuclear agreement, the incidence of covert action and retaliatory attacks between Washington and Tehran decreased. Reports of disruptive cyber operations against U.S. and Iranian infrastructure diminished, as Tehran focused more on domestic political opponents and regional adversaries, such as Israel and Saudi Arabia. Just as Operation Olympic Games provided Washington the ability to coerce Iran without direct military intervention, Tehran now engages in offensive cyber operations to project its regional power.

SAUDI ARABIA

No other country appears to have been the subject of as many offensive cyber operations from Iranian state-sponsored threat actors as Saudi Arabia. The two countries are ethnic (Arab vs. Persian), sectarian (Sunni vs. Shia), and above all geopolitical rivals, on opposing ends of bloody proxy wars in Iraq, Syria, and Yemen and fierce political battles in Bahrain and Lebanon. Relations between Tehran and Riyadh have often been tense since the 1979 Islamic Revolution, and formal diplomatic ties have been suspended intermittently due to political disputes. Most recently, in January 2016, Saudi Arabia closed its Tehran embassy after it was ransacked by an Iranian-government-sanctioned mob.

Saudi political and economic institutions have been compromised by Tehran for purposes of both espionage and disruption.

Since the start of Iran's cyber operations, Saudi political and economic institutions have been compromised by Tehran

for purposes of both espionage and disruption. In various reports on Iranian malware and credential theft campaigns—attempts to acquire passwords or account recovery information—Saudi Arabia has been one of the most common sources of victims and targets. This pattern reflects the two countries' profound geopolitical and ideological disputes (intent), and Saudi Arabia's continued vulnerabilities in cyberspace (opportunity).

Iran's August 15, 2012, attack on Saudi Aramco during the Muslim Eid holiday (and a similar attack against Qatar's RasGas Company two weeks later) is a prime example of how Iran uses offensive cyber operations to retaliate against foreign adversaries. As covert actions by foreign actors targeted Iran's nuclear and oil infrastructure, previously unknown groups began staging disruptive attacks against economic infrastructure in Saudi Arabia and the United States, portraying themselves as independent hacktivists motivated by nationalism and Islamic values.

Shamoon's message appeared clear: Iran may not always be able to defend itself against more advanced cyber capabilities, but it can impose substantial retaliatory costs against U.S. allies.

To avoid attribution, retaliatory acts were conducted using cutouts that provided them plausible deniability. In the Shamoon attack, known by the name given to the malware, tens of thousands of Saudi Aramco computers were compromised, causing tens to hundreds of millions of dollars in damage. One group, self-identified as the Cutting Sword of Justice, claimed responsibility for the attack, which overwrote the hard drives of Aramco computers with the image of a burning American flag, causing embarrassment to the company. Unlike the cyber operations conducted against Iran by foreign entities, the retaliatory attacks carried out by Tehran sought maximum visibility.

Initial analysis of the incident found that Shamoon was likely inspired by the Wiper malware that had targeted Iran in April 2012, given both destroyed stored data as a method of sabotage. Tehran was potentially motivated by retaliation for cyber operations against its oil production infrastructure. Shamoon's message appeared clear: Iran may not always be able to defend itself against more advanced cyber capabilities, but it can impose substantial retaliatory costs against U.S. allies.

The tit-for-tat cycle of covert destructive attacks and symbolic retaliation seen with Shamoon and Ababil reflects Iranian security tactics witnessed in offline hostilities. Between 2010 and 2012, for example, several Iranian nuclear scientists were assassinated under mysterious circumstances, allegedly by the United States or Israel.[82] In apparent retaliation, Tehran attempted, unsuccessfully, to assassinate Israeli officials in unexpected places like Georgia, India, and Thailand. This cycle, a recurrent theme in Iran's covert

actions, showed Tehran's ability to learn from attacks and retaliate in a similar fashion, providing a potential framework for understanding its signaling and motivations in conducting disruptive cyber operations.[83]

Compared to Iran's other adversaries (namely the United States and Israel), Saudi governmental and economic institutions have yet to sufficiently implement systems and protocols to increase national cybersecurity. Iranian actors have targeted a broad range of economic, military, and political institutions in Saudi Arabia—including Saudi Aramco and its foreign partners, the King Faisal Foundation, the Ministries of Commerce and Foreign Affairs, the Saudi Stock Exchange, and even Saudi Arabian human rights advocates. Researchers have documented multiple cases in which Saudi companies and organizations were compromised, in one event leading to the exfiltration of vast sums of archival proprietary data spanning multiple years from one industrial development corporation.[84]

Weak Saudi cyber defenses have not only made the country vulnerable to Iranian coercion but also made Riyadh a soft target for Tehran's retaliation against destructive cyber operations performed by third countries. If Iran cannot cause significant damage to the United States during times of conflict, then damaging the economic institutions of American allies will suffice.

The campaign of coercive pressure continues as well: the Saudi Ministry of Defense and other networks sustained DDoS attacks at the same time as the attack on the embassy.[85] When the Shamoon malware agent used in the Aramco incident reappeared in an updated form (labeled as Shamoon 2 by researchers) from November 2016 to January 2017, it destroyed databases and files belonging to both the government and private sector, including the General Authority of Civil Aviation, the Ministry of Labor, the Saudi Central Bank, and natural resource extraction companies.[86] Shamoon 2 contained references to Yemen and overwrote the victims' hard drives with an image of the drowned Syrian refugee child Alan Kurdi, once again signaling the attacks were retaliation for Saudi policies in Syria and Yemen.[87]

ISRAEL

One of the consistent pillars in Iran's foreign policy has been opposition to Israel's existence and support for anti-Israeli militant groups, such as Hezbollah, Hamas, and Palestinian Islamic Jihad. Despite this, however, Tehran has been far less successful in cyber operations targeting Israeli institutions for disruption and espionage. The documents used as bait in the Madi operation were commonly written in Hebrew or referenced Israeli security policies, and researchers have documented fifty-four compromised entities in Israel during that campaign.[88] During the conflict between Israel and Gaza

in the summer of 2014, known as Operation Protective Edge, authorities claimed that the Israel Defense Forces' infrastructure was targeted by DDoS attacks launched by a wide range of belligerents, including Tehran.[89] These DDoS attacks would align with the known capabilities of Iranian threat actors, including the tactics used against the United States and dissidents.

Despite a history of DDoS attacks and defacements of Israeli websites, Tehran's ability to inflict major costs on Israel through cyber operations has thus far been limited and perhaps diminishing.[90] Given the sophistication of Israel's cyber defense, Tehran has been forced to focus mainly on soft targets, for narrow espionage opportunities and the potential disruption of civilian resources in the event of conflict.

Iranian targeting of Israelis, like U.S. nationals, emphasizes individuals focused on Iran and regional policies. Tehran has engaged in spearphishing attempts against academic institutions, national security officials, diplomats, members of the Knesset, and Israeli aerospace companies. Similarly, Iranian actors have commonly created malicious domains that have emulated those owned by the American Israel Public Affairs Committee (AIPAC) and have targeted employees of both liberal and conservative Jewish organizations in the United States and elsewhere.

While Iran has had some success in compromising smaller civilian institutions, it has not visibly attempted to use these breaches coercively. The lack of immediate weaponization of breaches is demonstrative of how strategic calculations shape outcomes. The destruction of banking information or medical data over nonexistential challenges to the Islamic Republic is perhaps not worth inviting retaliation from Israel (a threat that Saudi Arabia lacks). Tehran's desire for signaling a credible retaliatory threat against Israel through offensive cyber operations may also be sufficiently served by the mere compromise of such institutions. Cyber capabilities have certainly not altered the power dynamics between Iran and Israel, and the difference in technical capacities likely shapes Iran's posture toward its adversary.

REGIONAL ALLIES AND ADVERSARIES

While Tehran's disruptive cyber operations in the region have primarily targeted Saudi Arabia, multiple Iranian threat actors have been observed targeting nearly every Middle Eastern, North African, and bordering country. For example, Magic Kitten successfully compromised victims across the Middle East and South Asia.[91] This pattern has been repeated during Madi and subsequent operations up to the present.

Cyber espionage has provided Tehran further insights about its often politically unstable neighbors. Iranian threat actors have shown a recurrent interest in the infrastructure of neighboring countries, including Afghanistan's National Radio, Ministry of Education, and government network.[92] Other indicators also suggest an interest in Pakistan's and Afghanistan's security and defense organizations.[93] Fictitious social media profiles and spearphishing campaigns have commonly targeted Iraqis, notably engineers within telecommunications networks and political elites. Iranian groups have also maintained an extremely active interest in the political institutions of Iraqi Kurdistan.[94]

In addition, multiple Iranian threat actors have engaged in spearphishing attempts against dozens of individuals affiliated with human rights organizations, political movements, and independent media outlets in Yemen, where Tehran is engaged in a proxy war with Saudi Arabia.[95] The Israeli cybersecurity company ClearSky found that 11 percent of the targets of one Iranian credential theft campaign (Rocket Kitten) in 2015 were connected to Yemen. These operations specifically support Iran's position in the Yemeni conflict, with recent attempts targeting prominent critics of the Houthis, the Shia Muslim group that Iran has been supporting in the country's civil war.

Iranian actors have also reportedly targeted Syrian opponents of President Bashar al-Assad's regime in limited cases, including exiled Syrian dissidents.[96] There has been speculation that Iran has also supported the offensive cyber operations of its traditional allies Syria and Hezbollah, notably after Syrian dissidents became the target of sustained malware campaigns starting in 2012. Yet there is only limited evidence of technical cooperation, and little reason why either would be dependent on Iran for capabilities.

While there are credible indications that Tehran has provided Syria traditional electronic warfare equipment, the Assad regime apparently didn't require extensive help with developing offensive cyber capabilities.

While there are credible indications that Tehran has provided Syria traditional electronic warfare equipment, the Assad regime apparently didn't require extensive help with developing offensive cyber capabilities. An indigenous ecosystem of hackers organized by Assad's relatives has proven effective at targeting the regime's opponents from early into the civil war. Small groups of hackers in Syria have typically used spyware that is popular among Arab hacking communities against opponents of Assad. Conversely, while little is known about Hezbollah's offensive cyber capabilities, in one 2015 report that described their malware and operations, the Lebanese group had seemingly outpaced its Iranian patron.[97]

The lack of external evidence of cooperation does not preclude other coordinated efforts or intelligence sharing, but basic cyber operations are easier than electronic warfare—such as signal jamming, radar collection, and signal location—or other military domains that require a defense industrial base.[98] None of the known capabilities or incidents involved specialized knowledge that required external support, and all have independent profiles on how their operations are conducted. Iranians have not used the same commodity spyware as Syrian groups, suggesting that pro-Assad groups owe more to local hacking scenes than other states. Moreover, Iran's lack of cooperation with allies or friendly foreign powers may reflect other factors influencing decisions to share resources. Allies still spy on allies: Iran could also want to withhold its toolkit to provide some oversight in contentious situations, such as monitoring the stability and loyalty of the Assad regime.

COMMERCIAL TARGETS

Unlike China, Iran has limited use for commercial espionage given its lack of an industrial production sector that could utilize stolen intellectual property. Iran's industrial espionage activities serve to boost its commodities industries and military technological prowess rather than its domestic manufacturing sector. Nor has Iran attempted to offset the impact of economic sanctions through large-scale financial crime, as North Korea appears to do.[99] Based on public reports and directly observed campaigns, the commercial entities targeted by Iranian threat actors typically fall into four categories:

- Aerospace and civil aviation
- Defense industrial base and security sector
- Natural resources and extractive industries
- Telecommunications firms

Evidence of Iran's interest in the theft of defense secrets comes from several cybersecurity reports, observed incidents, and U.S. indictments. Nima Golestaneh, an Iranian national extradited to the United States from Turkey, pleaded guilty to supporting the October 2012 hack of Vermont-based defense company Arrow Tech Associates in an operation to acquire copies of their weapon system simulations to sell the software to Iranian government and military entities.[100] This would prove to be a harbinger of later efforts.

In early 2014, in parallel to targeting Iranian women's development programs and others, one threat actor (Flying Kitten) impersonated a website for an aerospace systems conference to spread malware to defense contractors, a tactic still used against the industry

today. Another Iranian threat actor over the course of 2015 to 2016 repeatedly created phony corporate websites for Oshkosh Corporation, an American defense company, to capture credentials from its private internal business network, and continued to target aviation companies, including jet engine manufacturers and satellite companies. Reports of attempts of military espionage by Iranian threat actors are extremely common and include a broad set of industries, most notably aerospace technologies.

Yet these operations appear to have had limited success. Given their involvement in the defense industry, coupled with related concerns about Chinese industrial espionage, companies like Oshkosh prioritized information security in ways that NGOs have not. Consequently, while there is indication that employees are commonly targeted, even compromised, reports of the theft of highly sensitive defense secrets by Iran are rare.

The targeting of defense companies is also motivated by regional politics rather than solely theft of military technologies. Several defense industry companies targeted by Iranian threat actors, including Oshkosh Corporation, are substantially involved in providing security and military assistance to Saudi Arabia and other Gulf states. Many of the American companies—including Oshkosh Corporation—that were designated by the Iranian Ministry of Foreign Affairs in March 2017 under retaliatory human rights sanctions for their involvement with the Israeli military have also been targeted by Iranian cyber operations.[101]

As in other areas, it is difficult to derive intent purely from who was targeted or impersonated. In certain cases, it appears Iranian threat actors have compromised Middle East–based information technology consultants in pursuit of the governments or businesses who are their clients. These operations often target company employees based in the Middle East, potentially to acquire information on the military capabilities of rivals or access to other targets (such as supply-chain attacks). One more recent campaign masquerading as Boeing and Northrop Grumman appeared focused on Saudi Arabia's military and commercial aviation sectors.[102]

Similarly, Iran's targeting of telecommunications firms, banks, and civil aviation companies could provide them a foothold in critical infrastructure, one that could potentially cause substantial economic harm and even endanger lives. Thus far, however, Tehran appears to have used such targeting for reconnaissance purposes, mirroring other countries' cyber activities.[103] However, there are legitimate reasons to be concerned that Tehran's intention in targeting critical infrastructure is to hold social and economic assets in adversarial countries at risk in the event it needs to escalate or retaliate during conflict.

CHAPTER FOUR

IRAN'S INTERNAL TARGETS

The history of Iranian offensive cyber operations has demonstrated that the same threat actors responsible for espionage against the private sector engage in surveillance of human rights defenders, and with considerably more success, given the latter's resource constraints. Through the lens of such attacks, the relationship between Iran-originated cyber activities and the government as well as the motivations for such operations are made clearer. These communities foreshadow the tactics and tools that will be employed against other targets, and increased information will enable more effective education and mitigation strategies.

While the internet has afforded Tehran's security agencies new possibilities for surveilling and intercepting the communications of its citizens, concurrent information technologies also limit the reach of the state. Iran was one of the first countries in the Middle East to connect to the internet, and as a result over half of the population was frequently using the internet as of March 2017.[104] Iranian internet users have been quick to embrace social media and chat applications in large numbers as forums where there are more social freedoms.

As Iranian citizens have moved their communications to internet platforms hosted outside Iran and protected their communications from eavesdropping by using encryption, they have also evaded the more traditional means by which Iranian law enforcement and intelligence agencies perform surveillance.[105] Whereas local hosting providers and social media could be compelled to remove content and disclose account ownership information, platforms hosted outside Iran are beyond the direct reach of the state.

The Iranian government has sought to compel foreign firms to comply with requests for user data, without great success.[106] Domestic alternatives to foreign services, supported by the state under its national internet plan, have failed to attract significant adoption (Iranian officials themselves tend to use communication tools and social media applications developed in the United States).[107] Moreover, millions in the Iranian diaspora—many of whom left Iran because of state repression—live in countries with no security cooperation agreement with Tehran and are less inclined to communicate over insecure Iranian platforms. As a result, in contrast to the first two decades after the revolution, Iranians' communications and personal activities are increasingly out of the state's reach. This dynamic has fundamentally altered the nature of state controls.

The Iranian government has struggled to respond to the challenges posed by the internet to the state's information and communication monopoly. Among their first responses was mandatory content filtering, which entailed blocking access to any sites considered pornographic, antireligious, or politically subversive. With the increased availability of circumvention tools, however, filtering became less effective. Subsequently, basic offensive cyber operations, such as disrupting adversarial sites during the Green Movement, gave the regime the ability to reassert some control over information flows and project the illusion of the Islamic Republic's dominance over the internet.

Iranian cyber operations are highly adaptable as the online platforms and tools used by the public change. For example, after Iranians shifted to Telegram because of its unfiltered public chat feature and security claims, so too did the attention of Iranian threat actors. Alongside credential theft operations targeting Telegram users, one threat actor appears to have gone as far as mapping all the Telegram accounts connected with Iranian telephone numbers. This information-gathering operation had deeper ties to efforts to target the chat application's users and aligned with recurrent arrests of administrators from critical Telegram groups. This learning process is repeated elsewhere, including for mobile phones and Macintosh computers.[108]

Across discrete sets of threat actors and different periods of time, state-aligned offensive cyber operations routinely focus on similar classes of targets, primarily:

1. **Government officials**
2. **Reformist politicians**
3. **Media professionals**
4. **Religious minorities**
5. **Cultural figures**
6. **Opposition groups, terrorist organizations, and ethnic separatist movements**

GOVERNMENT OFFICIALS

Numerous Iranian threat actors have sought to compromise members of Hassan Rouhani's government, the administration of former president Mahmoud Ahmadinejad, and the state's bureaucratic institutions. The operations target not only government officials but also their relatives, including a sustained campaign directed against Rouhani's immediate and extended family (particularly his brother and adviser, Hossein Fereydoun).[109] Magic Kitten, the earliest known threat actor, from the outset engaged in intrusions of the Islamic Republic of Iran Broadcasting state television network and the Center for Strategic Research, the think tank research arm within the Iranian government's Expediency Council that was headed by Rouhani at the time.

Campaigns targeting the Iranian government are ongoing. The targeting of members of government—individuals that have already been vetted by the regime—reflects the importance of cyber surveillance as a tool of the hardline security establishment to monitor potential rivals for power and accrue sensitive information about people's lives that could potentially be used for blackmail or humiliation.

The Iranian Ministry of Foreign Affairs provides the most prominent and visible example of intergovernmental spying. Iranian diplomats have been frequent targets of spearphishing attempts conducted by IRGC-affiliated threat actors since the beginning of the Rouhani administration. These activities align with accusations in the hardline press that the nuclear deal betrayed Iranian interests.[110] The hacking attempts also mirror a history of arrests and pressure brought to bear on members of the diplomatic service accused of spying, including the August 2016 detention of Abdolrasoul Dorri-Esfahani, who served on Iran's nuclear negotiating team for the JCPOA.[111] Whereas diplomacy requires interacting with officials from foreign governments and external experts, these contacts can quickly be portrayed as engaging in espionage for foreign powers.

While Foreign Minister Javad Zarif and other figures have been the targets of social media defacements and threats, the campaigns conducted by the indigenous threat actors outlined in this report differ in their intent from simple hacktivism or vandalism. The objective is the collection of personal information from private accounts on international platforms and the monitoring of intimate political and professional networks of government officials.[112] These tactics include the typical credential theft attempts against personal email accounts seen elsewhere; however, special effort has been made to compromise government officials and their family members through elaborate deception and by using privileged resources.[113] Once compromised, those accounts have been then turned on their diplomatic contacts and peers. Zarif, and other senior diplomats, have been repeatedly impersonated and targeted by different IRGC-affiliated threat actors, as early as 2013 and as recently as February 2017.[114]

The diplomatic core is not the only target of intragovernmental spying: several cabinet officials of the Rouhani administration have had their personal email accounts targeted and compromised.[115] The cyber operations conducted by Iranian threat actors have extended beyond immediate members of government to target members of the Shia religious establishment, which undergirds the state's ideology and political affairs. Campaigns have compromised multiple individuals located in Qom, the center of Iranian religious matters, including hosts within the Center for Services of Islamic Seminaries and Islamic Propagation Office of Qom.

REFORMIST POLITICIANS

The accounts of Iranian reformers are a primary target for Iranian threat actors. Though reformers profess loyalty to the revolution and the Islamic Republic, they favor less state intervention in society and a less confrontational foreign policy, prioritizing the country's national interests before revolutionary ideology. Consequently, they have been increasingly purged from Iranian politics and there is a media and travel ban against their most prominent leader, former president Mohammad Khatami (who served from 1997 to 2005).[116]

After the Green Movement, associates of the former reformist presidential candidates Mehdi Karroubi and Mir-Hossein Mousavi were aggressively targeted by the regime to try and stifle their activities, even those who had fled under threat of prosecution. Unwilling to allow a repeat of the Green Movement, the regime tightened information controls in the run-up to the 2013 presidential election of Hassan Rouhani. Access to popular anticensorship tools was cut off, and internet speeds were throttled until after the election results were announced.[117] During this time, several Iranian actors began to concurrently target the accounts of Iranian political dissidents.[118] Offline, the families of international Persian-language media employees were harassed, and reporters inside Iran were subject to censorship or arrest.[119]

One of the first known cases of politically motivated hacking in Iran was when the blog of Mohammad-Ali Abtahi, the former vice minister of the Ministry of Culture and Islamic Guidance under Khatami, was defaced after he wrote about the arrest of bloggers in 2005.[120] Since then, Abtahi has been repeatedly targeted and impersonated by different Iranian threat actors in credential theft and social engineering operations.[121] Abtahi's experience is emblematic of such group's priority on reformists. Public figures in the reformist movement from all different segments of society and politics have been targeted. Not only the overtly repressed activists connected to Khatami, Karroubi, and Mousavi but former government officials, religious scholars, politicians, and professors.

The cyber operations against reformists have been broad, successful, and frequent. One threat actor maintained access to a computer used by a reformist cleric and a deputy at a prominent Iranian university for months, watching him conduct political operations and media interviews.[122] Similarly, in December 2015 the Facebook account of Gholam Ali Rajaee, a political activist close to former president Akbar Hashemi Rafsanjani, was used to spearphish the accounts of journalists and others.[123] The previous year, that same threat actor, Rocket Kitten, had also successfully compromised a number of former parliament members and other reformists in the diaspora, some of whom were later arrested.

The cyber operations against reformists have been broad, successful, and frequent.

Young activists mobilizing for reformists were targeted with malware and credential theft operations in the lead up to the February 2016 parliamentary election, particularly those connected to female candidates. The targeting often aligns with offline pressure from the IRGC and Intelligence Ministry: when the office of one reformist close to Rouhani was raided in May 2017, he was targeted in repeated spearphishing attempts. Despite the ascent of moderates to more positions of power, reformists remain a primary target of the government's cyber capabilities.

MEDIA PROFESSIONALS

Iranian cyber operations have repeatedly focused on journalists working with reformist media outlets and international satellite broadcasters that fall immediately outside the strict state-sanctioned narratives. Multiple Iranian threat actors conducted numerous credential theft attempts, using fake service notifications, against Iran-based foreign correspondents and Iranian journalists working for prominent publications such as *Shargh* and the Iranian Labor News Agency. Similarly, freelance reporters inside Iran are frequently compromised through fictitious personas that send them malware purporting to be news content. These campaigns have often targeted publications that would later be closed and journalists who would be detained by Iranian security forces. These incidents are also often timed with elections, normally periods when the government has more aggressively prosecuted journalists.

The case of Jason Rezaian, the *Washington Post*'s former correspondent in Iran, is illustrative of state-aligned threat actors' focus on foreign press working in Iran. Before his arrest on July 22, 2014, and eighteen-month imprisonment by the IRGC, Rezaian had been the target of concerted intrusion efforts by Flying Kitten. The threat actor attempted to

compromise Rezaian's Hotmail and Gmail accounts on multiple occasions through credential theft attempts launched from fictitious security addresses; these attempts warned of spam being sent from the account and of other hacking threats. The emails were not themselves technically sophisticated, as the English used in the messages was poor and the approach was amateurish. However, the behavior in these incidents was unique in that Rezaian's accounts were singled out from a small set of targets several months prior to his arrest.

RELIGIOUS MINORITIES

Iranian religious minorities are obvious targets of the Iranian security forces, most notably adherents of the highly persecuted Baha'i faith, who have long been accused of promoting conspiracies against the Islamic government.[124] With the widespread adoption of the internet, the Baha'i leadership, based mostly in the United States and Haifa, Israel, enjoyed new organizational and communication opportunities otherwise denied to them offline. Those same technologies, however, also gave the Iranian state new capabilities for intelligence gathering and propaganda dissemination against the Baha'i.

In April 2014, the Gmail account of a former director of external affairs for the U.S. Baha'i organization was accessed from inside Iran. The director had a history of international advocacy on behalf of the Baha'i Assembly that included testifying before Congress on the status of religious minorities in Iran. This made her a natural target for Iran. Fictitious LinkedIn and social media profiles previously employed against the U.S. defense industry, including one claiming to be former UN ambassador John Bolton, were used to target the Baha'i director with credential theft attempts posing as reports on religious persecution.

The ongoing targeting of the Baha'i and the defacement of their sites underscores the Iranian regime's concern with organizations it perceives as subversive.

Prominent members of the faith, including the diaspora relatives of imprisoned Baha'i leaders in Iran, continue to be subjected to sustained cyber operations. Similarly, cutout groups as recently as February 2017 defaced Baha'i sites with pro-regime propaganda coinciding with events such as the anniversary of the Islamic Revolution. The ongoing targeting of the Baha'i and the defacement of their sites underscores the Iranian regime's concern with organizations it perceives as subversive and its use of disruptive attacks to buttress the ideological agenda of the state.

The religious targets of Iranian cyber operations have not been limited to aggressively marginalized groups such as the Baha'is but also include recognized religious communities such as Christians, Jews, Zoroastrians, and Sunni Muslims. In one example, a mainstream Jewish community leader in Tehran was compromised through malware and surveilled as he went about coordinating events and managing a local religious publication. Still other spearphishing campaigns have routinely targeted evangelical Christian converts, atheists, or new age religious sects. More broadly, a malware campaign posing as information on the persecution of Christian converts was sent to human rights organizations, and fictitious profiles have posed as religious minorities to infiltrate evangelical Persian-language networks.[125]

CULTURAL FIGURES

Iran-originating spearphishing campaigns have also targeted Iranian cultural figures—including artists, musicians, comedians, cartoonists, and satirists—regardless of whether they reside in Iran or abroad.

These campaigns have included the targeting and compromise of social media and email accounts for the Germany-based musician Shahin Najafi, multiple pop stars that left Iran after the Islamic Revolution, a Persian-Israeli singer, and an Iranian-born female metal musician based in the United States, among others. There have also been intrusions into devices and accounts associated with less prominent underground artists inside Iran and networks of fictitious social network profiles connected with Iranian death metal rock bands and hip-hop groups. These themes of targeting famous pop musicians and their staff—both inside Iran and abroad—are recurrent and do not focus solely on individuals critical of the establishment.

Iranian security forces have publicly acknowledged their operations to identify individuals involved in "immoral behavior" online. In January 2016, several Iranian fashion models popular on social media were arrested for their activities online and forced to delete their accounts, an effort labeled by the IRGC as Operation Spider. At the same time, the arrests of employees of the foreign-based AAA Music television channel led to their social media accounts being defaced with a message, purportedly from the Ministry of Intelligence, about the illegality of the network. In interviews with and public statements by those rounded up in Operation Spider, these individuals were commonly operating openly, and the defacements were conducted after they were forced to hand over passwords.

Operation Spider was not the first of its kind: the activities of Flying Kitten suggest an earlier interest in surveillance of the Iranian fashion industry.[126] In early 2014, the threat

actor compromised the computer of a social media model that was popular for portraying a fashionable lifestyle without wearing the state-mandated hijab.[127] After the intrusion she retreated offline, stopped logging on to modeling sites, and deleted her Facebook account. Her image was also appropriated for further operations against other communities. The opaque nature of campaigns such as Operation Spider obscures how Iranian authorities track down people like online models. However, incidents such as the Flying Kitten compromise and the infiltration of LGBT-support networks and sex worker social media communities by others suggest a relationship between both efforts.

OPPOSITION GROUPS, TERRORIST ORGANIZATIONS, AND ETHNIC SEPARATIST MOVEMENTS

Despite its labeling of civil dissent as a threat to national security, Iran does face real threats of terrorism and organized crime from nonstate actors, evidenced by the self-proclaimed Islamic State's June 2017 attacks on its parliament and the mausoleum of former Iranian supreme leader Ayatollah Ruhollah Khomeini. While documentation of Iranian cyber operations by international researchers has typically assumed that all domestic targets of intrusion campaigns are political dissidents, a small portion of these campaigns focus on areas in which law enforcement hacking has become internationally normalized, chiefly in the collection of evidence and intelligence on violent terrorist activities and financial crime.

For instance, Iranian threat actors have actively sought to compromise the digital operations of Sunni jihadi movements through credential theft, malware, and other intrusions.[128] To compromise Islamist organizations, Iranian actors have leveraged bait documents and messages in Persian and Arabic and posed as media organizations such as Al Jazeera and Al Arabiya. Flying Kitten attempted to spread malware by posting comments on Al Arabiya's Facebook page purporting to promote jihadism. These intelligence efforts have targeted jihadi groups across the Middle East and North Africa, Pakistan, and Afghanistan, including the Islamic State and al-Qaeda, while focusing on Iraqi and Persian-language groups.[129]

Security-related cyber operations extend as well to fringe political organizations that have previously engaged in hostilities against the Islamic Republic.[130] Iranian threat actors have successfully compromised individuals affiliated with front groups for Mojahedin-e Khalq (MeK) opposition group, including the Iranian American Society of Texas and the Simay Azadi television station. These intrusions provided access to private Facebook discussion groups and intra-organizational planning for MeK rallies, Telegram channels,

and MeK television programming. Given the MeK's past disclosures on Iran's nuclear program, which the organization has claimed were conducted through an in-country network of collaborators, these activities also constitute a counterespionage program.

Iranian threat actors also maintain a significant focus on disenfranchised ethnic minorities advocating for greater autonomy. One recurrent target has been Baluchi groups, a Sunni Muslim population located in both Iran and Pakistan. The news outlets and social media accounts of Baluchi militant organizations, such as Jundallah, have repeatedly been targeted by Tehran. These operations include breaching multiple Jundallah affiliated sites as early as July 2010 to push malware to their visitors, a "watering hole attack" designed to surveil violent separatists that would be of interest to Iranian security agencies.[131] In other cases, from a different threat actor, Jundallah was targeted using malware hosted on domains purporting to be related to the Free Syrian Army and sent in emails claiming to provide documentation of attacks against the IRGC.

Tehran has also devoted considerable resources to cyber operations targeting Kurdish organizations inside Iran and abroad. Malware samples from April 2015 targeted the Free Life Party of Kurdistan (PJAK), a militant Iranian faction of the Marxist-Leninist Kurdistan Workers' Party (PKK).[132] The same threat actor appears to have successfully compromised a Kurdish satellite television station, Newroz TV, aligned with the PKK. Newroz TV was also compromised by the Flying Kitten malware in 2014, indicating an overlap not only in the threat actors' mandates but also in their exact targets. Still other groups have used fictitious LinkedIn profiles to connect to representatives of the Kurdistan Regional Government in Iraq. Judging from computer names and other indicators, many more of those compromised by Iranian malware were in Iran's Kurdistan province, while others were found in Iraqi Kurdistan, or among the Kurdish population in Europe.

The internet has increased the Iranian government's opportunities for surveillance and repression against foreign-based operations.

CIVIL SOCIETY

The internet has facilitated communication and organization between Iranians and foreign and diaspora organizations, but it has also increased the Iranian government's opportunities for surveillance and repression against foreign-based operations.

Though many foreign civil society organizations have been the subject of sustained attempts at infiltration and disruption by Iran, few appear to have incurred attacks of such persistence and aggression as those against the Eurasia Foundation, an NGO in Washing-

ton, DC, that conducts development programs in former Soviet countries, the Middle East, and China. As part of its Iran-focused social development programs, the Eurasia Foundation in October 2009 launched the Khorshid School of Entrepreneurship, which promoted women's entrepreneurship through distance learning courses and the creation of professional networking opportunities.

Eurasia Foundation's programs and organizational history connect closely with Khamenei's fears of a Velvet Revolution. It would later launch several more online Persian-language programs covering a range of issues, from social entrepreneurship to family law. The first intrusion attempt occurred shortly after an article was published in the hardline Iranian newspaper *Kayhan* in February 2014. It accused the Eurasia Foundation of engaging in social engineering by establishing networks of women and teachers to foment grassroots economic, political, and social pressure on the regime—all under the direction of the U.S. Agency for International Development and the U.S. State Department. Ten days after the article appeared, Flying Kitten began its spearphishing campaign against the Eurasia Foundation. For the next two years, the Eurasia Foundation would continue to be the target of malware, credential theft, and social engineering by diverse threat actors with diverse strategies.[133]

The campaign against the Eurasia Foundation is emblematic of Iran's long and ongoing history of cyber operations against U.S.-based NGOs. U.S. think tanks have been a focus of interest, with targets such as the American Enterprise Institute and the Council on Foreign Relations singled out by multiple Iranian threat actors. The same Iranians that targeted the Eurasia Foundation in December 2015 also impersonated the network administrators at multiple Washington, DC, foreign policy institutions critical of the Iranian government to compromise employees.

Nor are these efforts directed only at Iran's detractors. Organizations advocating improved relations with Iran or nonpolitical researchers have been routinely targeted—the common denominator appears to be simply a policy interest in Iranian affairs.

CONCLUSIONS AND PRESCRIPTIONS

While Iran's offensive cyber operations have required modest resources to develop, they have allowed Tehran to project itself as an emerging cyber power able to cause significant harm to its adversaries. The country's security establishment has used these resources to signal to domestic and international audiences its ability to confront political subversion and retaliate against attacks on its infrastructure. These actions have brought international attention to Iran as a considerable force, perhaps beyond its actual capabilities, but have been ambiguous enough to allow Tehran to portray itself as a victim of the coercive measures of foreign states.

As judged from evidence of coordination between security agency actions and observed cyber operations, the campaigns of Iranian threat actors almost certainly have a direct relationship with government entities, specifically the Islamic Revolutionary Guard Corps and the Ministry of Intelligence. Given this alignment and collaboration, Iranian threat actors are described here as state-sponsored. However, since the threat actors are commonly private contractors in small security companies, these relationships are sometimes nebulous and the operators are not integrated into the state's forces.[134]

Iranian cyber operations often reflect law enforcement behavior normalized by other countries in response to advancing information technologies, such as the hacking of devices to wiretap encrypted internet communications. International standards forums and telecommunication equipment vendors have legitimized the expectation of lawful interception of communications, and the Iranian government faces similar challenges of providing domestic security against terrorist organizations and crime that other coun-

tries encounter. These interests are expressed frequently in campaigns, which include the documentation of persistent targeting of militant organizations—both domestic and regional—that are hostile to the Iranian government, including Baluchi separatists and the Islamic State.

With the exception of Saudi Arabia, Iran appears to have had little success in compromising hardened government institutions or well protected organizations. After two decades of cyber crime, governments and private corporations have developed security policies and maintain collaborative relationships with external security organizations (for example, computer emergency readiness teams, or CERTs) that allow them to defend against attacks. In the office environment, companies can provide dedicated technical resources, exercise centralized control over devices, offer user education, and install protective network equipment that reduces risk. Such resources enable the private sector and governments to respond to threats and improve awareness collectively as a community.

Private threat intelligences companies and governmental agencies, such as the FBI's Cyber Watch (CyWatch), provide corporations with regular reports on common security risks, including information on the attacker's documented tools and infrastructure. The FBI has produced industry notifications on Iranian intrusion activities based on reports sourced from the private sector, and U.S. government entities have identified Iranian malware through information supplied from threat intelligence companies. When multiple computers in the Voice of America's Persian service were infected by Iranian malware named Infy, the agent's origin was identified by network administrators through a private report generated by a threat intelligence company that was made available to the agency.[135]

Such resources are not readily available to individuals—especially those residing in Iran—who find themselves alone and unprepared when targeted by even the most unsophisticated threat actors. While American banks quickly invested in countermeasures that limited the effectiveness of subsequent DDoS attempts in Operation Ababil, Persian-language social media platforms and media organizations subject to the same attacks commonly turned off services rather than pay thousands of dollars in bandwidth costs.[136] One FBI notice sent to the private sector even documented fictitious profiles that were also used to target the Baha'i community.[137] However, the FBI and cybersecurity companies do not commonly notify at-risk communities of threats to their safety and privacy. This divergence and exclusion represents the differences in opportunities afforded to nongovernmental and noncorporate targets of state-aligned threat actors.

The increased attention to user security by information technology companies in recent years has directly benefited the targets of Iran. Persian-language digital literacy and

information security education programs have been developed through foreign assistance to cater to at-risk audiences, teaching concepts such as password management and how to recognize social engineering. Widely available account features such as two-factor authentication, which requires a user to provide a code sent through text message or an application to log into accounts, have demonstrably made it more difficult for Iranians to conduct credential theft. Private companies, such as Google and Cloudflare, as well as government funders, have supported DDoS-mitigation services that provide civil society organizations with enterprise-level defense resources to protect against such attacks at no cost, leading to a marked decrease in their frequency.

As a result, a well-educated user with two-factor authentication and an iOS device is a more difficult target for Iranian threat actors to compromise. However, while technological options for protecting accounts and devices have improved in recent years, in the end the biggest vulnerability remains the user.

Attempts to forecast the future of Iranian cyber operations are constrained by the secrecy on the part of the Iranian state about its activities and an uncertain geopolitical climate. Like most countries, Tehran does not appear to have a clear doctrine as to when it will engage in disruptive operations and retaliate in cyberspace. Nor is it likely to. In line with its asymmetric strategies in traditional warfare, Tehran has often benefited from ambiguity. This may explain why it denies operations attributed to it, as well as why it did not immediately incorporate threat actors into the military apparatus.

Having been the target of sustained cyber espionage and destructive attacks, Iran is bound to seek the same capabilities used against it. These capabilities provide Tehran opportunities to impose costs during potential hostilities. While Iran may not appear able to perform synchronized multistage attacks wherever it would like, it can repeatedly hammer away at soft targets in campaigns of attribution. Renewed hostilities between Iran and the United States could be expected to involve the targeting of vulnerable economic, civilian, and governmental services with data destruction, DDoS, and other disruptive attacks. Under current perceptions of Iranian offensive cyber capabilities, it is unclear that it would be prepared and able to launch attacks against the power grid or industrial control systems, such as those conducted against Ukraine.[138] Instead, attacks would follow the path of least resistance—targeting state and local governments rather than federal infrastructure, or unprepared sectors that have not been previously targeted such as transportation and logistics rather than the financial services. Attempts by one

Having been the target of sustained cyber espionage and destructive attacks, Iran is bound to seek the same capabilities used against it.

Iranian to meddle with a local New York dam and other reports about the compromise of state agencies are demonstrative of the abundance of opportunities for Iran to retaliate against the United States.[139]

Moreover, although Iran has been described as a rational actor, it is not unitary, as the overlapping operations and intragovernmental surveillance conducted by the Ministry of Intelligence and IRGC demonstrate.[140] The motivations, coordination, and authorization of Iranian state-aligned campaigns may differ from the policy position of other branches of government, and the use of offensive cyber capabilities is less visible to observers than the mobilization of troops. Iran's security apparatus can easily conduct hostilities in cyberspace without the consent or awareness of the rest of the government.

Disruptive activities conducted by Iranian threat actors have decreased overall since the interim nuclear deal signed in November 2013—known as the Joint Plan of Action framework. The rhetoric of government and military officials has also evolved over time. In recent years, particularly under the Rouhani administration, fewer blusterous statements have been made regarding Iran's cyber operations.[141] While Tehran is less likely to engage in disruption of American or European infrastructure amid current circumstances, it has engaged in cyber espionage and will continue to do so. The perceived success of previous campaigns has solidified the principle of offensive cyber operations as an effective means for Iran to continue to conduct espionage and surveillance against regional adversaries and political opponents.

Yet Iran will continue to be limited by resource constraints for the foreseeable future. Tehran has rarely appeared able to conduct large-scale exfiltration of classified business and government data, differing, for example, from Chinese efforts to steal Boeing's industrial secrets or extensive databases from the U.S. Office of Personnel Management.[142] What's more, the threshold of difficulty for compromising such targets will increase over time, and it is unclear whether Iranian capabilities will improve proportionally.

Iran's massive brain drain, with many of its brightest engineers leaving for political and economic reasons, imposes further constraints on the development of its cyber capabilities. Iran's minister of science, research and technology estimated that 150,000 highly talented people emigrate from Iran every year, a $150 billion annual economic loss.[143] When Iranian engineers leave for Silicon Valley and Europe, the country's capacity for effective offensive and defensive cyber operations goes with them.

In the absence of a historical comparison of Iranian cyber operations, new incidents or the rise of new groups is often incorrectly perceived as a dramatic improvement to capacity. Despite systemic challenges stemming from bureaucratic dysfunction and underinvestment in cybersecurity, Iran has the potential to foster more effective operations.

Attempts by the government, universities, and the private sector to create a professional cybersecurity community, such as hosting Capture the Flag tournaments, will inevitably result in a deeper talent pool. Observing other nation-state actors provides a set of benchmarks that can be a reliable indicator of improvement or change in posture, including:

- coordination of threat actors, more consistent improvement to domestically produced malware, and the development of purpose-built tools that could suggest the consolidation of capability, specialization of personnel, and even incorporation into the state;
- investments in operational security, ranging from reducing the exposure of information on operators to increased investment in concealment (such as Magic Kitten's relay network);
- improvements in background research and foreign language abilities within operations, such as more personalization of social engineering attempts, that would reflect the inclusion of nontechnical support staff; and
- execution of operations that include zero-day exploits or target core infrastructure (for example, compromising network devices, routing protocol hijacks, and telecommunications signaling manipulation), suggesting more investment in resources for systemic cyber operations.

Despite Iran's current lack of technical sophistication, simple means can still be effective at imposing political and economic costs, as evidenced by Russia's successful compromise and subsequent leaking of the internal communications of Democratic Party institutions and operatives before the 2016 U.S. election. Some of the most damaging materials used in the operation came via a simple breach of a Gmail account, an opportunity available to anyone. This also reinforces the challenge of discerning intent—what initially appears as espionage can later turn into an attack.[144]

Given Iran's dispersed ecosystem of threat actors, deterring Tehran from engaging in offensive cyber operations is as challenging as other efforts to address security issues involving the country. Cyber activities are less likely to lead to regional destabilization than are offline Iranian threats, and historically, Tehran's disruptive attacks against non-Iranian targets have been retaliation during hostilities rather than instigation toward new conflicts. To maintain credibility at a time when Western surveillance activities are publicly exposed through leaked confidential documents, effective policy responses need to differentiate espionage or signaling from sabotage or the infringement of human rights, actions that violate international norms. It is also important to recognize that Iranian offensive cyber operations do not require technology transfers or the support of other states. Members of Iranian threat actors—primarily low-level software developers

working within a small number of companies—will continue to be tough to identify, prosecute, and punish.

Naming and shaming may chill participation in state-aligned operations, especially among talented individuals looking to travel outside the country or study abroad. However, it is unclear whether those publicly identified with Operation Ababil or other campaigns have changed their involvement after being outed. Moreover, the loosely connected and small groups are not cost-effective targets for retaliatory cyber operations. In the end, Iran maintains a large enough pool of sufficiently capable programmers to conduct basic campaigns. Therefore, while exposing Iranian cyber operations and operators may degrade and delay the development of better cyber capabilities, it will not fully deter Iran.

POLICY APPROACHES TO IRAN'S CYBER THREAT

This leaves a select number of policy options, primarily (1) utilizing existing frameworks for targeted sanctions or indictments, (2) improving information sharing on threats across communities, and (3) supporting initiatives to improve information security.

The comprehensive sanctions regime against Iran is unlikely to substantially interfere with its development of offensive cyber capabilities. Iranians commonly use servers outside the country, typically hosted on networks in Europe and Russia that provide service to other cyber crime networks (bulletproof hosting) or registered using false information.[145] Since the resources necessary to improve capacity are organizational and professional development rather than computers or infrastructure, there are few technological items or services that could potentially be deterred. Furthermore, overly broad sanctions regimes that attempt to constrain malicious cyber activities would be more likely to have substantial collateral damage on the free flow of information to Iran, as Iranian civil society has widely argued.

The U.S. Treasury Department's Office of Foreign Assets Control maintains targeted programs that can be brought to bear against international entities that augment Iran's capacity for surveillance against its population.

Where sanctions are appropriate, the U.S. Treasury Department's Office of Foreign Assets Control maintains targeted programs that can be brought to bear against international entities that augment Iran's capacity for surveillance against its population (Executive Order 13606[146]) and those responsible for

cyber operations against American infrastructure (Executive Order 13694).[147] Sanctions and other financial mechanisms could be used to deter foreign countries or other actors from providing support to Iranian offensive cyber operations. Executive Order 13606 offers an example in its authority to designate any entity, whether in Iran or elsewhere, that has facilitated the Iranian government in its "computer and network disruption, monitoring, and tracking." While the order focuses on human rights, similar language could focus on Tehran's attacks against critical infrastructure and espionage. The narrowly tailored extension of these authorities could help ensure that Iran's cyber operations do not benefit from technology transfers or foreign assistance as Tehran expands its security and commercial ties, especially to countries such as Russia and China.

Additionally, the Justice Department has issued indictments against Iranians implicated in disruptive campaigns (the same individuals allegedly responsible for Operation Ababil were also designated under Executive Order 13694) and has successfully obtained the extradition from a third country of a hacker involved in the theft of military secrets.[148] Because of the small operational footprint of the groups, targeted sanctions or legal proceedings are more symbolic than disruptive, but few other opportunities exist to impose consequences on individuals who participate in operations.

Given the level of rudimentary nature of its cyber operations, a purely political or legal response that is focused solely on deterring Iran would be ineffective toward addressing national cybersecurity risks. Any system that can be breached by Iranian groups is equally susceptible to others with similar sets of motivations, notably North Korea and Hamas. An effective policy response to the threats posed by Iran must focus on securing critical infrastructure overall.

Information sharing has been one of the most common strategies pursued by the United States, Europe, and the private sector to reduce the effectiveness of Iranian cyber operations. After the Aramco attack, the United States used its superiority in monitoring and attributing Iranian activities to strengthen intelligence relationships with its Arab allies in the Persian Gulf.[149] This is an immensely valuable resource that should be extended where possible, and further support can be provided to regional allies. Similarly, the FBI has provided notifications to and facilitated information sharing with the private sector on specific Iranian campaigns. These efforts can be expanded to include more partners and to provide data to civil society organizations.

Unlike traditional security issues, private individuals are more exposed to cyber operations owing to the transnational and virtual nature of threats. This brings in more stakeholders, and increases the burden on individuals to protect themselves from crime and espionage. Responsibility to protect those users rests equally on the private sector and governments. Fortunately, internet platforms and communications services, like

Facebook and Google, have played a positive role in providing the tools to help individuals defend against attacks—even going so far as notifying users when they have been targeted by state-aligned campaigns, including those from Iran. These initiatives raise the bar for attackers and should be seen within tech companies as a core obligation of keeping at-risk users safe.

Discussions about securing dissidents would be incomplete without highlighting the pioneering role of the United States government and European development agencies in providing secure communications tools to activists—often referred to as the Internet Freedom agenda. Government funding has provided early stage investment for researchers and developers to produce prototypes and deployable products to protect activists and civil society that would not be the focus of the private sector. A significant proportion, if not majority, of Iranians that bypass the censorship regime do so using safe and reliable tools funded by the State Department and Broadcasting Board of Governors. Both have also supported the development of encryption tools such as Signal that have even been adopted by tech companies within their own messaging applications, demonstrating the importance of Internet Freedom as a public-private cooperation.

The United States and European Union should continue to promote programs and norms on internet access and cybersecurity that prioritize the free and secure flow of information against challenges from countries such as Iran, China, and Russia. Aside from funding for civil society, this includes promotion of democratic values within internet governance frameworks, such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the International Telecommunications Union (ITU). This also highlights the importance of domestic policy on Internet Freedom efforts: proposals to weaken information security products such as encrypted messaging applications would harm individuals in countries where rule of law is weak and backdoor access in communications networks is commonly repurposed for repression.

As the history of Iranian offensive cyber operations demonstrates, the same actors responsible for espionage against the private sector engage in surveillance of human rights defenders, and with considerably more success, owing to the targets' resource constraints. These at-risk communities provide a canary for the tactics and tools that will be employed against other targets, and increased information exchange will enable more effective education and mitigation strategies for all. Policymakers have long understood that the changes that will lead Iran to be a productive member of the international community will come from within. The safety and security of the Iranian civil society organizations and democratic voices targeted by government cyber operations should be recognized and protected as the critical stakeholders within cybersecurity and foreign policy discussions that they are.

GLOSSARY

Campaign: A set of activities carried out by threat actors for some particular purpose.

Credential theft: The process of stealing credentials associated with online platforms, such as passwords or account recovery information.

Distributed denial-of-service (DDoS): An attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.

Offensive cyber operations: Cyberspace operations intended to project power by the application of force in or through cyberspace.

Sinkhole: Redirection of malicious internet traffic so that it can be captured and analyzed by security researchers.

Spearphishing: A targeted attack that uses a deceptive email to trick the recipient into performing some kind of dangerous action for the adversary.

Supply chain attack: The strategic compromise of a particular entity, such as a vendor, with the intent to indirectly compromise another, primary target, such as the vendor's clients.

Threat actor: An individual or group involved in malicious cyber activity.

Watering hole attack: The compromise of a selected website in order to stage intrusion attempts through malware to the visitors of the site.

NOTES

1 "Department of Defense Dictionary of Military and Associated Terms," Federation of American Scientists, amended February 15, 2016, https://fas.org/irp/doddir/dod/jp1_02.pdf.

2 The authors cannot identify under what level of authority the attacks are authorized and whether Iran will professionalize such operations under state security forces. However, they can say with high confidence that such activities are coordinated with the Iranian government. See Jason Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks," Atlantic Council, February 22, 2012, http://www.atlanticcouncil.org/publications/issue-briefs/beyond-attribution-seeking-national-responsibility-in-cyberspace.

3 This material will posted on "Iran Threats," Github, https://iranthreats.github.io.

4 GReAT, "The Madi Campaign – Part I," SecureList, July 17, 2012, https://securelist.com/blog/incidents/33693/the-madi-campaign-part-i-5.

5 David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

6 The preparation for Operation Olympic Games was substantial. Intelligence agencies in the United States and Israel obtained confidential information about the specific configuration of the centrifuge controllers in Natanz, built a test environment based on comparable hardware seized from Libya, and then deployed the malware agent through human assets inside Iran to reach computers disconnected from the internet. These operations were sustained over years. Later versions of Stuxnet exploited several previously unknown vulnerabilities and sought to strategically infect other computers in Iran in the event that they were connected to the Natanz systems.

7 Iran's National Computer Emergency Response Team, Kaspersky Lab, and CrySyS Lab.

8 Ellen Nakashima, Greg Miller, and Julie Tate, "U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say," *Washington Post*, June 19, 2012, https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html.

9 "Iran Says Detected 'Massive Cyber Attack:' State TV," Reuters, June 21, 2012, https://www.reuters.com/article/us-iran-cyber-nuclear/iran-says-detected-massive-cyber-attack-state-tv-idUSBRE85K1EA20120621.

10 "Iran 'Fends Off New Stuxnet Cyber Attack,'" BBC News, December 25, 2012, http://www.bbc.com/news/world-middle-east-20842113.

11 Communications Security Establishment Canada, "SNOWGLOBE: From Discovery to Attribution," accessed December 4, 2017, a presentation discussing the French malware otherwise known as Babar, available at http://www.spiegel.de/media/media-35683.pdf.

12 Karim Sadjadpour, "Reading Khamenei: The World View of Iran's Most Powerful Leader," Carnegie Endowment for International Peace, March 10, 2008, http://carnegieendowment.org/files/sadjadpour_iran_final2.pdf.

13 "15 June 2009 – Tehran – Iran – Protest continued – Protesters Are Going to Freedom (Azadi Sq)," YouTube video, 1:02, posted by "saeidkermanshah," June 15, 2009, https://www.youtube.com/watch?v=9_hr7G4At84.

14 A common example of this collaboration is when Twitter had planned to conduct maintenance after the June 2009 election. The State Department requested that the company delay the downtime in consideration of the protests. See Sue Pleming, "U.S. State Department Speaks to Twitter Over Iran," Reuters, June 16, 2009, http://www.reuters.com/article/us-iran-election-twitter-usa-idUSWBT01137420090616. More aggressively, in an opinion piece in the *Wall Street Journal*, a former under secretary of state and an assistant secretary of defense advocated for increased funding for communications tools and foreign broadcasting efforts with the express intent to "undermine the regime in Tehran." See James K. Glassman and Michael Doran, "The Soft Power Solution in Iran," *Wall Street Journal*, January 21, 2010, http://www.wsj.com/articles/SB10001424052748704541004575011394258630242.

15 The day before the March 2012 Iranian parliamentary elections, employees of the BBC were unable to access their email owing to a DDoS attack attributed to Iran. The Mujahedin-e Khalq has also claimed that when its former encampment in Iraq, Camp Liberty, was attacked in February 2013, its websites were subjected to a sustained DDoS attack designed to interfere with reporting. "Cyber-attack on BBC Leads to Suspicion of Iran's Involvement," BBC News, March 14, 2012, www.bbc.com/news/technology-17365416.

16 One document used as bait in the malware campaign appears to be a secret letter from the Ministry of Intelligence to members of the religious establishment in Qom concerning the protests over subsidies. Another displayed maps in Tehran describing protest routes toward Azadi Square, mirroring the activities on the ground. The malware agent would arise again over time in attempts to compromise the American defense industrial base in May 2014, and again in the Shamoon 2 attacks.

17 *Black Tulip: Report of the Investigation Into the DigiNotar Certificate Authority breach* (Delft: Fox-IT BV, 2012), https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2012/08/13/black-tulip-update/black-tulip-update.pdf. In a confidential document on its own ability to monitor secure traffic, the UK Government Communications Headquarters (GCHQ) provides an account of the DigiNotar event, discovered in the course of its own espionage on Iran. GCHQ asserts that an Iranian intelligence agency added a specific rule in an internet router that forced Google's traffic through an alternative route inside the country. "Profiling SSL and Attributing Private Networks," GCHQ, December 28, 2014, https://edwardsnowden.com/2015/01/07/profiling-ssl-and- attributing-private- networks/.

18 Akbar Ganji, "Iran's Green Movement Five Years Later – 'Defeated' But Ultimately Victorious," Huffington Post, accessed December 4, 2017, https://www.huffingtonpost.com/akbar-ganji/iran-green-movement-five-years_b_5470078.html.

19 The most conspicuous and potentially only counterexample could be Oilrig, which across a multiple year history appears primarily focused on foreign targets and has not been publicly linked to attacks against Iranians.

20 Figures for both the United States and Iran are kept secret, however, a leaked intelligence budget for the 2013 provides some insight into how cyber operations are funded. Barton Gellman and Ellen Nakashima, "U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents Show," *Washington Post*, August 30, 2013, https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html.

21 "Minister: Iran Faces 500 Daily Cyber Attacks," Khabar Online, November 10, 2012, http://english.khabaronline.ir/detail/183007.

22 "We just want to monitor (enemies') cultural and social moves in cyber," quoted in "IRGC to Set Up Division to Defend Iran Against Cyber Threats," Sahar TV, October 16, 2012, http://english.sahartv.ir/news/irgc-to-set-up-division-to-defend-iran-against-cyber-threats-1638.

23 "Statement by Foreign Ministry Spokesman for Indictment of US Justice Department Against Seven Iranian Citizens," Iranian Ministry of Foreign Affairs, March 26, 2016, http://mfa.gov.ir/index.aspx?fkeyid=&siteid=1&pageid=2122&newsview=385735.

24 Alexander Gostev, "What Is Flame Malware?," Kaspersky Lab, accessed December 5, 2017, https://www.kaspersky.com/flame.

25 "US Cyber Attack on Iranian Oil Ministry Foiled," FARS News Agency, May 26, 2015, http://en.farsnews.com/print.aspx?nn=13940305001092.

26 "Iran Unveils 12 Cyber Products," FARS News Agency, December 14, 2013, http://en.farsnews.com/newstext.aspx?nn=13920923001322.

27 "Iranian Internet Infrastructure and Policy Report: Special Edition – The Rouhani Review (2013–15)," Small Media, 2015, https://smallmedia.org.uk/sites/default/files/u8/IIIP_Feb15.pdf; Office of the Press Secretary, "Fact Sheet: Cybersecurity National Action Plan," White House, press release, February 9, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan; and Steve Morgan, "Bank of America's Unlimited Cybersecurity Budget Sums Up Spending Plans in a War Against Hackers," *Forbes*, January 27, 2016, https://www.forbes.com/sites/stevemorgan/2016/01/27/bank-of-americas-unlimited-cybersecurity-budget-sums-up-spending-plans-in-a-war-against-hackers/#694de941264c.

28 Barbara Slavin and Jason Healey, "Iran: How a Third Tier Cyber Power Can Still Threaten the United States," Atlantic Council, July 29, 2013, http://www.atlanticcouncil.org/publications/issue-briefs/iran-how-a-third-tier-cyber-power-can-still-threaten-the-united-states.

29 Recent espionage incidents targeting U.S. State Department employees have been described in the press as "attacks" that sought to "jab at the United States and its neighbors without provoking a military response." Despite the implication of aggression, the incident appeared to be motivated for espionage. David E. Sanger and Nicole Perlroth, "Iranian Hackers Attack State Dept. via Social Media Accounts," *New York Times*, November 24, 2015, http://www.nytimes.com/2015/11/25/world/middleeast/iran-hackers-cyberespionage-state-department-social-media.html.

30 Michael N. Schmitt, "Cyber Operations and the Jus Ad Bellum Revisited," *Villanova Law Review* (December 2011): 569–605.

31 Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013). U.S. officials have acknowledged that international law applies to actions in cyberspace as well. Patrick Tucker, "NSA Chief: Rules of War Apply to Cyberwar, Too," Defense One, April 20, 2015, http://www.defenseone.com/technology/2015/04/nsa-chief-rules-war-apply-cyberwar-too/110572/.

32 Carmen-Cristina Cîrlig, "Cyber Defence in the EU: Preparing for Cyber Warfare?," briefing, European Parliament, October 2014, http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf.

33 As has been documented in intelligence material leaked by Edward Snowden: "Iran – Current Topics, Interaction With GCHQ," Intercept, February 10, 2015, https://theintercept.com/document/2015/02/10/iran-current-topics-interaction-gchq/.

34 International law also differentiates interference, nonviolent operations such as propaganda, and psychological operations, so long as they are not sufficiently coercive. Schmitt, "Cyber Operations and the Jus Ad Bellum Revisited."

35 Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge: Cambridge University Press, 2018).

36 Ibid.

37 The tools and resources developed by Tehran have been almost uniformly described by outside investigators as unsophisticated, particularly in comparison with malware produced by other state and nonstate actors. The information security company Mandiant affirmed this observation in a 2014 report: "Mandiant's observations of suspected Iranian actors have not provided any indication that they possess the range of tools or capabilities that are hallmarks of a capable, full-scope cyber actor. They rely on publicly available tools and capitalize solely on Web-based vulnerabilities—constraints that suggest these cyber actors have relatively limited capabilities." See: Mandiant, "M-Trends 2014 Annual Threat Report: Beyond the Breach by Mandiant, a FireEye Company," accessed December 5, 2017, https://www2.fireeye.com/fireeye-mandiant-m-trends-report.

38 For example, former representative Peter Hoekstra speculated at a U.S. House hearing that Iran's advances in cyberwarfare came from the "cooperation they have with Russia." Other former and current officials have commented, often on background, that Russia was a potential partner in warfare. For the subcommittee hearing on Iran's support terrorism worldwide, see the following: "Iran's Support for Terrorism Worldwide," Foreign Affairs Committee, March 4, 2014, https://foreignaffairs.house.gov/hearing/joint-subcommittee-hearing-irans-support-for-terrorism-worldwide/. Elsewhere, claims have been made by lesser known cybersecurity companies, but these analyses have been flawed and not well accepted. For more on these flawed analyses, see: Collin Anderson, "Bears and Kittens, and Startup Cybersecurity Companies," Medium, May 18, 2017, https://medium.com/@collina/bears-and-kittens-and-startup-cybersecurity-companies-5c8e037ea75c.

39 Steve Stecklow, "Exclusive: Huawei Partner Offered U.S. Tech to Iran," Reuters, October 25, 2012, http://www.reuters.com/article/us-huawei-iran/exclusive-huawei-partner-offered-u-s-tech-to-iran-idUSBRE89O0E520121025; and "Iran and Russia Announce Plans for Cyber Security Cooperation," YouTube video, 2:03, posted by "PressTV News Videos," March 15, 2017, https://www.youtube.com/watch?v=NaCukjiECWM.

40 This could be either indicative of the ceiling of Iran's capabilities or reflective of Iran not facing the sort of existential threat that would provoke it to use any latent resources in its arsenal. The former appears more likely.

41 Rocket Kitten and Flying Kitten are examples of how the line demarcating intrusion groups is not always clear. The structural similarities of certain intrusion tools and the reuse of lesser known infrastructure indicate that parts of Flying Kitten and Rocket Kitten may have had a common heritage, including common members and shared tools; see: Collin Anderson, "Flying Kitten to Rocket Kitten, A Case of Ambiguity and Shared Code," Iran Threats, December 5, 2017, https://iranthreats.github.io/resources/attribution-flying-rocket-kitten/. In the Shamoon 2 campaign, McAfee attributed unusual errors to the "involvement of different groups/individuals with different skills, whereas in 2012 we believe one group was responsible for the attack." See: Christiaan Beek and Raj Samani, "The State of

Shamoon: Same Actor, Different Lines," McAfee, April 25, 2017, https://securingtomorrow.mcafee.com/executive-perspectives/state-shamoon-actor-different-lines/.

42 The authors associate Rocket Kitten with the IRGC due to its involvement in post-arrest hacking. For more on Rocket Kitten, see: "Rocket Kitten 2 – Follow-Up on Iran Originated Cyber-Attacks," *ClearSky Cybersecurity* (blog), September 1, 2015, http://www.clearskysec.com/rocket-kitten-2. For more on Oilrig, see: Robert Falcone and Bryan Lee, "The OilRig Campaign: Attacks on Saudi Arabian Organizations Deliver Helminth Backdoor," Palo Alto Networks, March 26, 2016, https://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/.

43 Reportedly, the attacker found sensitive passwords saved in a file named "Administrator Passwords." See: Sam Jones, "Cyber Warfare: Iran Opens a New Front," *Financial Times*, April 26, 2016, http://app.ft.com/cms/s/15e1acf0-0a47-11e6-b0f1-61f222853ff3.html?sectionid=companies. No official numbers have been provided on the economic loss, and in its annual review report for the year, Aramco downplayed the impact of the attack. "Shaping Tomorrow: 2012 Annual Review," Saudi Aramco, April 10, 2013, http://www.saudiaramco.com/en/home/news-media/publications/corporate-reports/annual-review-2012.html.

44 The caveat attending this statement is that it is possible more incidents and actors have yet to be disclosed.

45 Based on a Freedom of Information Act request by the authors to the Broadcasting Board of Governors on cybersecurity incidents related to Iran, which returned details of the attack, involving compromising the VOA's account through impersonation with falsified documents sent through a fax.

46 The intruders were able to find a weakness in a web development server for the Bethlehem, Pennsylvania, location, and doing so then gave them access to the internal corporate network. Benjamin Elgin and Michael Riley, "Nuke Remark Stirred Hack on Sands Casinos That Foreshadowed Sony," *Bloomberg*, December 10, 2014, http://www.bloomberg.com/news/articles/2014-12-11/nuke-remark-stirred-hack-on-sands-casinos-that-foreshadowed-sony.

47 Symantec Security Response, "Shamoon: Back From the Dead and Destructive as Ever," *Symantec Connect* (blog), November 30, 2016, https://www.symantec.com/connect/blogs/shamoon-back-dead-and-destructive-ever; "From Shamoon to StoneDrill: Wipers Attacking Saudi Organizations and Beyond," Kaspersky Lab, July 3, 2017, https://securelist.com/files/2017/03/Report_Shamoon_StoneDrill_final.pdf.

48 ITSec Team, one of the companies cited in the indictment, has a known track record as the developer of a web penetration testing product (Havij Pro), and is attributed in a number of vulnerability disclosures and tools for controlling remote systems that have been made available to security researchers. The infrastructure used in the attacks even remains publicly exposed to the internet years after its use.

49 Seth Hardy, et al., "Targeted Threat Index: Characterizing and Quantifying Politically-Motivated Targeted Malware," *23rd USENIX Security Symposium* (2014): 527–41, https://www.usenix.org/node/184440.

50 Jacob Appelbaum, Aaron Gibson, Claudio Guarnieri, et al., "NSA Preps America for Future Battle," *Der Spiegel*, January 17, 2015, http://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409.html.

51 Curiously, when Google disclosed the spearphishing campaigns that Magic Kitten was involved in, it noted to the *New York Times* that there was a relationship between the operation and the DigiNotar incident. Nicole Perlroth, "Google Says It Has Uncovered Iranian Spy Campaign," *Bits* (blog), *New York Times*, June 12, 2013, https://bits.blogs.nytimes.com/2013/06/12/google-says-it-has-uncovered-iranian-spy-campaign/.

52 "CrowdStrike Global Threat Report: 2013 Year in Review," CrowdStrike, January 2014, https://scadahacker.com/library/Documents/Threat_Intelligence/CrowdStrike%20-%20Global%20Threat%20Report%202013.pdf.

53 The lack of clarity in the slides is also compounded by the age of the document and could reflect an arrangement that is no longer in effect. However, within observations of activity, there does appear to be a clustering of victims, with some samples of the malware agent specifically used to compromise Lebanese and Qatari victims, but not Iranians or other targets of exclusive interest to Iran.

54 Members of the infamous Ashiyane hacking community and others commonly broke into Arabic media and U.S. government sites with political messages, such as protesting alternative names for the Persian Gulf, Western perceptions of Islam, nuclear rights, the administration of George W. Bush, and the crimes of other countries—often in broken English and always bearing attribution. In a few cases these campaigns were sustained over longer periods of time and were intended to make a point, especially when it came to Israeli and Saudi targets. "Al Khaleej Newspaper Website Hacked," Gulf News, March 7, 2017, http://gulfnews.com/news/uae/general/al-khaleej-newspaper-website-hacked-1.106195; Zone-H mirror page, "fdfhome.gsfc.nasa.gov hacked. Notified by Mafia Hacking Team," archived on May 26, 2005, http://www.zone-h.org/mirror/id/7494752; Zone-H mirror page, "lvis.gsfc.nasa.gov hacked. Notified by Ashiyane Digital Security Team," archived on August 11, 2005, http://www.zone-h.org/mirror/id/2757516; Zone-H mirror page, "technology.jpl.nasa.gov hacked. Notified by hamid," archived on December 28, 2005, http://www.zone-h.org/mirror/id/3183620.

55 Aspects of this can be found in the individuals documented in Dan McWhorter, "APT1: Exposing One of China's Cyber Espionage Units," Mandiant, 2013, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

56 Sheera Frenkel, "Meet the Mysterious New Hacker Army Freaking Out the Middle East," BuzzFeed News, June 24, 2015, https://www.buzzfeed.com/sheerafrenkel/who-is-the-yemen-cyber-army; and Brian Bartholomew and Juan Andres Guerrero-Saade, "Wave Your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks," *Virus Bulletin Conference* (October 2016): 1–11, https://cdn.securelist.com/files/2016/10/Bartholomew-GuerreroSaade-VB2016.pdf.

57 In its indictment, it even went as far as claiming that one individual had received relief from mandatory military service in return for participation. *United States of America v. Ahmad Fathi et al.*, unsealed March 24, 2016, https://www.justice.gov/opa/file/834996/download. The attribution for the campaigns and indication of the American intelligence community's early attribution of the participants are evident in screenshots from a presentation on the NSA's CyberCOP program from April 2013, which describes the scale of the DDoS attacks and the infrastructure behind the botnet in its later phases of operation. See: "CyberCOP," presentation, CyberCOP Product Manager, April 11, 2013, http://www.ndr.de/ratgeber/verbraucher/cybercop100.pdf.

58 Zone-H mirror page, "www.karroubi.ir hacked. Notified by Sun Army," archived on February 17, 2010, http://www.zone-h.org/mirror/id/10269967.

59 Florian Egloff, "Cybersecurity and the Age of Privateering: A Historical Analogy," Cyber Studies Program Working Paper no. 1 (Oxford: University of Oxford, March 2015), http://www.politics.ox.ac.uk/materials/centres/cyber-studies/Working_Paper_No.1_Egloff.pdf.

60 Richard Barger, "There's Something About Mahdi," Threat Connect, July 23, 2012, https://www.threatconnect.com/blog/there-is-something-about-mahdi/; and "Summary of Mortalkombat.com," Wayback Machine Internet Archive, accessed September 17, 2017, https://web-beta.archive.org/web/20080415000000*/m0rtalkombat.com.

61 Flying Kitten has also established Pars Security (Pars Pardazesh Hafez Shiraz). The FBI had made similar allegations not only for the culprits of Operation Ababil, companies named Mersad and ITSecTeam, but also in the Arrow Tech Associates theft. The FBI's indictment claims that two other individuals

formed a company, Andisheh Vesal Middle East Company, to steal software on behalf of the Iranian government. *United States of America v. Mohammed Saeed Ajily and Mohammed Reza Rezakhah*, unsealed July 17, 2017, https://www.justice.gov/opa/press-release/file/982106/download.

62 For those on the ground the threats posed are more complex and multifaceted. For example, Iranian telecommunications firms appear to have cooperated with the government in order to provide access to the recovery and two-factor authentication codes sent by text. These then allowed access to Google, Telegram, and other accounts on foreign platforms.

63 The most significant counterevidence of state-alignment is that when the Infy group was disclosed by Palo Alto in May 2016, the domains used in the communications of the malware were filtered by the censorship apparatus, blocking access to those victims. There are explanations for this action that would not conflict with the theory that Infy was acting on behalf of the government, including that the censorship was intended to hide evidence of the operation from the Iranian public.

64 Specifically, we observed direct interactions between the Iranian state and the groups Charming Kitten, Flying Kitten, Magic Kitten, and Rocket Kitten. More tenuous links exist for Infy based on this criteria.

65 "Rocket Kitten: A Campaign With 9 Lives," Check Point Software Technologies Ltd., November 9, 2015, https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf.

66 The incident was orchestrated by a threat actor who had registered domains under cmprus1394[@]mail[.]ru and teymurov1984[@]gmail[.]com, which impacts a vast network of espionage and criminal activity.

67 *United States of America v. Behzad Mesri, a/k/a "Skote Vahshat,"* unsealed November 21, 2017, https://www.justice.gov/usao-sdny/press-release/file/1013001/download.

68 Robin Wright, "An American Hostage in Iran – Again," *New Yorker*, October 30, 2015, http://www.newyorker.com/news/news-desk/an-american-hostage-in-iran-again.

69 A dual national who had previously worked with a foreign broadcaster was arrested two weeks after his email was also compromised after a phishing attempt. According to one account, the attacker attempted to extract a ransom to keep the victim's private information, which was ignored. Then, after the arrest, the accounts were again used to target others.

70 "Iranian Billionaire Babak Zanjani Sentenced to Death," BBC News, March 6, 2016, http://www.bbc.com/news/world-middle-east-35739377.

71 These intrusions reflected a studied understanding of Sorinet's operations and included names such as "Baharak Zanjani" that appear on the corporate registrations of the company's subsidiaries but are believed to be false identities. See article in Farsi, Young Journalists Club, February 2, 2013, http://www.yjc.ir/fa/news/4744029/%D9%85%D8%A7%D8%AC%D8%B1%D8%A7%DB%8C-%D8%AE%D9%88%D8%A7%D9%87%D8%B1%D8%A7%D9%86-%D8%AC%D8%B9%D9%84%DB%8C-%D8%A8%D8%A7%D8%A8%DA%A9-%D8%B2%D9%86%D8%AC%D8%A7%D9%86%DB%8C.

72 Iranian security and intelligence agencies have however frequently used blackmail and humiliation to intimidate or coerce individuals, including BBC Persian journalists. It is possible that material compromised through intrusions has been used for political manipulation, as this would be difficult to observe without acknowledgement from the victim. For examples of blackmail threats, see: Elise Knutsen, "Iranian Agents Blackmailed BBC Reporter With 'Naked Photos' Threats," *Arab News*, November 19, 2017, http://www.arabnews.com/node/1195681/media.

73 Based on monitoring of known registration information used by Charming Kitten, suspicious domains include saudi-government[.]com and saudi-haj[.]com.

74 "Verfassungsschutzbericht 2015" (in German), German Ministry of the Interior, June 2016, https://www.verfassungsschutz.de/de/download-manager/_vsbericht-2015.pdf; "Phishing uden fangst: Udenrigsministeriet under angreb" (in Danish), Center for Cybersikkerhed, Ministry of Defense,

January 2016, https://fe-ddis.dk/cfcs/CFCSDocuments/Phishing%20uden%20fangst.pdf; and "Security Warning-Shamoon 2," CERT.sa, accessed December 5, 2017, http://www.cert.gov.sa/index.php?option=com_content&task=view&id=714&Itemid=0.

75 U.S. National Security Agency, "Iran – Current Topics, Interaction With GCHQ," Intercept, written January 8, 2007, published February 10, 2015, https://theintercept.com/document/2015/02/10/iran-current-topics-interaction-gchq/.

76 David Crawford, "U.N. Probes Iran Hacking of Inspectors," *Wall Street Journal*, May 19, 2011, http://www.wsj.com/articles/SB10001424052748704281504576331450055868830. The IAEA would later be targeted by an Iranian hacktivist group, calling itself Parastoo, in November 2012, when a web server was compromised, and the information on its employees was posted online, with the implied threat of another Aramco attack. For Parastoo's statement, see http://cryptome.org/2012/11/parastoo-hacks-iaea.htm.

77 First disclosed by Kaspersky Lab and Seculert in July 2012; see "The Madi Campaign – Part I," SecureList. While researchers noted the religious implications of the inclusion of the word "mahdi.txt" in the malware's operations, other versions appeared to include other Persian names and words such as "otahare." It seems more likely that the inclusion was not meant as a religious declaration.

78 Later attributed by Cylance as Operation Cleaver. Unnamed U.S. government officials had characterized the breach as "carried out by hackers working directly for Iran's government or by a group acting with the approval of Iranian leaders," see: "U.S. Says Iran Hacked Navy Computers," *Wall Street Journal*, September 27, 2013,https://www.wsj.com/articles/us-says-iran-hacked-navy-computers-1380314771.

79 ClearSky, "Jerusalem Post and Other Israeli Websites Compromised by Iranian Threat Agent CopyKitten," *ClearSky Cybersecurity* (blog), March 30, 2017, http://www.clearskysec.com/copykitten-jpost/; and "Brief Summary, 2016 Report on the Protection of the Constitution: Facts and Trends," German Ministry of the Interior, 2016, https://www.verfassungsschutz.de/embed/annual-report-2016-summary.pdf.

80 Hillary R. Clinton investigation records, https://vault.fbi.gov/hillary-r.-clinton. See in particular Document 3, an FBI Interview from February 3, 2016.

81 Direct observation of the targets of the Charming Kitten group. The email addresses and names of those targeted in these campaigns appear to have been sourced from the Podesta emails released by WikiLeaks.

82 Alan Cowell, "Blast Kills Physics Professor in Tehran," *New York Times,* January 12, 2010, http://www.nytimes.com/2010/01/13/world/middleeast/13iran.html; and Dan Raviv and Yossi Melman, *Spies Against Armageddon: Inside Israel's Secret Wars* (BookBaby, 2014).

83 The attempted bombings occurred February 13, 2012, one month after the assassination of Mostafa Ahmadi Roshan (on January 11, 2012) and four years after the death of Imad Mughniyah (on February 12, 2008).

84 First hand observation of the activities of the Charming Kitten group, similar to the successful operation described in the Operation Cleaver report by Cylance.

85 "Top Daily DDoS Attacks Worldwide: Saudi Arabia," Digital Attack Map, January 2, 2016, http://www.digitalattackmap.com/#anim=1&color=0&country=SA&list=1&time=16802.6&view=map.

86 "From Shamoon to StoneDrill," Kaspersky Lab.

87 "'Sophisticated' and 'Genius' Shamoon 2.0 Malware Analysis," Coding and Security, December 3, 2016, https://www.codeandsec.com/Sophisticated-CyberWeapon-Shamoon-2-Malware-Analysis.

88 Symantec Security Response, "The Madi Attacks: Series of Social Engineering Campaign," *Symantec Connect* (blog), July 17, 2012, https://www.symantec.com/connect/blogs/madi-attacks-series-social-engineering-campaigns.

89 Kirk Soluk, "DDoS and Geopolitics – Attack Analysis in the Context of the Israeli-Hamas Conflict," Arbor Networks, August 5, 2014, https://www.arbornetworks.com/blog/asert/ddos-and-geopolitics-attack-analysis-in-the-context-of-the-israeli-hamas-conflict/.

90 Although one Israeli intelligence official has stated that "they are not the state of the art, they are not the strongest superpower in the cyber dimension, but they are getting better and better," disclosing that Iran continues to attempt to compromise Israeli systems. Ari Rabinovitch, Tova Cohen, and Dan Pleck, "Iran's Hacking Ability Improving: Israeli General," Reuters, October 31, 2017, https://www.reuters.com/article/us-cyber-summit-padan/irans-hacking-ability-improving-israeli-general-idUSKBN-1D02O0.

91 U.S. National Security Agency, "(U) Fourth Party Opportunities: I Drink Your Milkshake," *Der Speigel*, published January 17, 2015, http://www.spiegel.de/media/media-35684.pdf.

92 Directly collected indicators from a sinkhole of malware associated with the Infy group.

93 For example, in Check Point's Rocket Kitten report, included in the group's infrastruture were domains mirroring the Afghan Ministry of Defense. Similar domains and targets can be found later that are connected to the same group.

94 Directly collected indicators from the Infy group; discussed further in relation to Iran's targeting of ethnical minority groups.

95 Directly collected indicators from the Flying Kitten group. The recipients of these spearphishing campaigns included a wide range of journalists and political groups, such as the Coordination Council of Yemen Revolution Youth, Yemen Center for Human Rights, Social and Democracy Forum of Yemen, and Yemen Parliamentarians Against Corruption. The leaked NSA slide indicates that Magic Kitten also breached Yemeni computers, but the nature of the targets is unclear, and the document predates the onset of the civil war in Yemen.

96 "Group5: Syria and the Iranian Connection," Citizen Lab, August 2, 2016, https://citizenlab.org/2016/08/group5-syria/.

97 "Volatile Cedar: Threat Intelligence and Research," Check Point Software Technologies Ltd., March 30, 2015, https://www.checkpoint.com/downloads/volatile-cedar-technical-report.pdf.

98 One striking and related claim made in November 2017 was that the Iranian threat actor Oilrig had compromised Lebanese politicians in order to run an information operation in support of Hezbollah in the 2018 general election. See: Patrick Saint-Paul, "Téhéran sponsor d'un piratage massif contre le gouvernement d'Hariri" (in French), *Le Figaro*, November 26, 2017, http://www.lefigaro.fr/international/2017/11/26/01003-20171126ARTFIG00124-teheran-sponsor-d-un-piratage-massif-contre-le-gouvernement-d-hariri.php.

99 Michael Corkery and Matthew Goldstein, "North Korea Said to Be Target of Inquiry Over $81 Million Cyberheist," *New York Times*, March 22, 2017, https://www.nytimes.com/2017/03/22/business/dealbook/north-korea-said-to-be-target-of-inquiry-over-81-million-cyberheist.html?mcubz=0; "Lazarus Under the Hood," Kaspersky Lab, April 3, 2017, https://securelist.com/files/2017/04/Lazarus_Under_The_Hood_PDF_final.pdf.

100 *United States of America v. Mohammed Saeed Ajily and Mohammed Reza Rezakhah*.

101 "Iran Sanctions 15 U.S. Firms, Citing Human Rights Abuses and Israel Ties," Reuters, March 26, 2017, http://www.reuters.com/article/us-iran-usa-sanctions-idUSKBN16X0DL.

102 Jaqueline O'Leary, Josiah Kimble, Kelli Vanderlee, and Nalani Fraser, "Insights Into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and Has Ties to Destructive Malware," FireEye, September 20, 2017, https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html.

103 Ryan Gallagher, "The Inside Story of How British Spies Hacked Belgium's Largest Telco," Intercept, December 13, 2014, https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/.

104 "Iran Telecoms, Internet Report 2016-2017," *Financial Tribune*, April 26, 2017, https://financialtribune.com/articles/economy-sci-tech/63062/iran-telecoms-internet-report-2016-17.

105 For example, the mobile chat applications and voice over internet protocol (VOIP) services, such as Viber, Skype, and Telegram, that became popular replacements for standard telephony and text messaging bypass the lawful interception capacities traditionally embedded in phone systems.

106 One significant example is Telegram, which has reached over 40 million users in Iran as of 2017. As a result of its use of encryption, it is not susceptible to the filtering of specific content or keywords. While both Iranian authorities and Telegram have never been fully forthcoming about their relationship, it is clear that the former has attempted to incentivize and threaten Telegram into complying with requests for the removal of content—including briefly blocking the service in October 2015. While it appears that Telegram does take down pro–Islamic State content, it has not thus far complied with other requests.

107 Collin Anderson, "How Iran Is Building Its Censorship-Friendly Domestic Internet," *Backchannel* (blog), *Wired*, September 23, 2016, backchannel.com/how-iran-is-building-its-censorship-friendly-domestic-internet-11db69aae96d.

108 Joseph Menn and Yeganeh Torbati, "Exclusive: Hackers Accessed Telegram Messaging Accounts in Iran—Researchers," Reuters, August 2, 2016, http://www.reuters.com/article/us-iran-cyber-telegram-exclusive-idUSKCN10D1AM.

109 Fereydoun has been the target of a corruption investigation, which has been perceived as an attempt to undermine Rouhani. Regardless of the legitimacy of these claims, the attempts against Fereydoun began early in Rouhani's first term and targeted his family. This extended into impersonating Zarif to target Fereydoun and vice versa. The long-term focus suggests the targeting was related to politics rather than the criminal investigation.

110 Aresu Eqbali, "Back Home, Iran's Leader Tries to Sell Nuclear Deal," *Wall Street Journal,* July 16, 2015, http://www.wsj.com/articles/back-home-irans-leader-tries-to-sell-nuclear-deal-1437081590.

111 Aresu Eqbali and Asa Fitch, "Iran Accuses Man Involved in Nuclear Deal Negotiations of Spying," *Wall Street Journal*, August 28, 2016, https://www.wsj.com/articles/iran-accuses-man-involved-in-nuclear-deal-negotiations-of-spying-1472416462.

112 Hanif Kashani, "Zarif, Attacked But Unscathed," Iran Wire, September 17, 2013, https://en.iranwire.com/features/2665/.

113 Such as the use of mobile phone interception to capture login credentials for Telegram and Google accounts. In other cases, elaborate ruses appeared to be set up based on private political information in order to convince the target to run malware.

114 Based on data acquired through forensic investigations of Flying Kitten and Charming Kitten's credential theft campaigns.

115 On April 19, 2016, the Google and Facebook accounts of Shahindokht Molaverdi, at that time Iran's vice president for Women and Family Affairs, were compromised by Rocket Kitten in order to conduct a spearphishing campaign against women's rights activists.

116 The ban was imposed in February 2015. "Rouhani and Judiciary Clash Over Ban on Publishing Images of Former President Khatami," Center for Human Rights in Iran, December 21, 2015, https://www.iranhumanrights.org/2015/12/khatami-media-ban-and-etelaat-newspaper/.

117 Collin Anderson, "Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran," arXiv.org, June 18, 2013, http://arxiv.org/abs/1306.4361.

118 Specifically, Flying Kitten, Infy, and Magic Kitten.

119 "Iran Accelerates Crackdown on Media and Dissidents Prior to Election," International Campaign for Human Rights in Iran, June 10, 2013, https://www.iranhumanrights.org/2013/06/iran_election/.

120 Parthisan, "Abtahi's Blog Was Hacked for Revealing Torture Details," Persian Students in the United-Kingdom, January 2, 2005, hosted by Internet Archive, https://web.archive.org/web/20050123083526/http://www.persianstudents.org/archives/001269.html.

121 Based on observation of the Rocket Kitten's social engineering attempts against foreign human rights activists that appeared to use a breached account belonging to Abtahi.

122 Based on data acquired from a malware command and control server found through forensic investigation of Flying Kitten activity.

123 Gholam Ali Rajaee, "Warning!" (in Farsi), December 27, 2015, http://www.gholamalirajaee.blogfa.com/post/1152/%D9%87%D8%B4%D8%AF%D8%A7%D8%B1.

124 "Iran: Baha'is Educating Their Youth Is a 'Conspiracy' Against the State," Baha'i World News Service, July 27, 2011, http://news.bahai.org/story/843. In response to this persecution, the Baha'i community has become particularly adept at using the internet for international advocacy and countering exclusion, including offering online distance learning classes from the Baha'i Institute for Higher Education.

125 The Infy malware agent, as directly observed in January 2016.

126 Shima Shahrabi, "Iran's New Criminals: Fashion Models," Iran Wire, February 2, 2016, https://en.iranwire.com/features/7058.

127 Based on data acquired from a malware command and control server found through forensic investigation of Flying Kitten activity.

128 FireEye (through its iSIGHT Partners) has also noted that threat actors focused on the Islamic State as the militant group was expanding its territory across Iraq, an interest expressed by the threat actors well before 2015. David E. Sanger and Nicole Perlroth, "Iranian Hackers Attack State Dept. via Social Media Accounts," *New York Times*, November 24, 2015, http://www.nytimes.com/2015/11/25/world/middleeast/iran-hackers-cyberespionage-state-department-social-media.html.

129 In one case a shared computer in Erbil, Iraq, used by a Kurdish supporter of a Jordanian jihadi figure was compromised through the malware, which was delivered as personal pictures sent by a fictitious female social network profile. The same group maintained phishing sites with hard-coded references to Facebook pages associated with the Islamic State's "Ministry of Information," Tunisian Islamic Awakening, Lashkar-e-Khorasan (Pakistan), and al-Qaeda affiliates, among other Islamist movements. This targeting was broad, but more effort was spent on Persian-language or Iran-oriented actors, targeting Facebook pages as small as one with five members and one public post, a "Salafe Kurdistan" page.

130 The operations reflect old rivalries from the Islamic Revolution being played out, as Flying Kitten sought access to accounts and sites associated with Marxist-Leninist Fedaian and other Communist parties as well.

131 Some of the first observed operations of the Infy group targeted Taftaan News Agency and the Jonbeshe Moqavemate Mardomie Iran separatist group, and compromised computers in the province of Sistan and Balochistan over the course of several years. Shortly after the suspected time of intrusion, at least one of the affected blogs warned its visitors that an old email address connected to the site had been compromised by Iranian intelligence agencies. The following day the administrators closed the site, claiming technical issues.

132 Several Infy malware samples had names such as "pjak.pps" and other references to Marxist ideologies (such as "kargar.pps," or "worker").

133 For example, current and former employees of the organization, both with the Iran Program and general operations staff, have been engaged by several fictitious personas on LinkedIn and Facebook, including the persona "Victoria Roberts," the LinkedIn profile name described earlier as connecting predominantly with defense companies. The existing networks of these profiles reflect a specific interest in the American foreign policy establishment, international development programs, and the defense industrial base.

134 Healey defines "state-integrated" as the "national government integrates third-party attackers and government cyber forces, with common command and control." This still allows for informal coordination with external parties so long as the government remains in control. While Iranian threat actors receive tasking from the government, there is little indication that any of them are formal members of the security forces.

135 Based on a Freedom of Information Act request by the authors to the Broadcasting Board of Governors on cybersecurity incidents related to Iran.

136 David M. Faris and Babak Rahimi, eds., *Social Media in Iran: Politics and Society After 2009* (Albany, NY: SUNY Press, 2015).

137 An FBI notice sent to private industry on May 29, 2014, described a similar set of personas that expanded on the iSIGHT Partners' (now FireEye) Operation Newscaster report that was released a few days prior. While iSIGHT Partners identified fourteen accounts of American or European background, the FBI provided a list of fifty-six unique personas, of which fifteen had family names that appeared to be Persian and had not been identified in the previous report. The accounts identified by the FBI have been since deleted, but appeared to have been Iran-focused. Federal Bureau of Investigation, "FBI Notification: Malicious Cyber Actors Targeting U.S. Government Networks and Employees," Public Intelligence, June 23, 2014, https://publicintelligence.net/fbi-cyber-targeting-gov-networks/.

138 John Hultquist, "Sandworm Team and the Ukrainian Power Authority Attacks," *Threat Research* (blog), FireEye, January 7, 2016, https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html.

139 "A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case," *New York Times*, March 25, 2015, https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html. FireEye (which owns Mandiant) has described multiple cases of "Iran-based network reconnaissance activity," including unauthorized intrusions into several U.S. state government agencies. "FireEye Releases Annual Mandiant Threat Report on Advanced Targeted Attacks," FireEye, April 10, 2014, http://investors.fireeye.com/releasedetail.cfm?ReleaseID=839454.

140 Alex Vatanka, "The Iranian Industrial Complex: How the Revolutionary Guards Foil Peace," *Foreign Affairs*, October 17, 2016, https://www.foreignaffairs.com/articles/iran/2016-10-17/iranian-industrial-complex.

141 For example, when Iranian state–aligned media have covered such issues in recent years, it has typically been through republishing English-language reports without substantial further comment or by reporting on denials by the government, such as when Mashregh News covered Citizen Lab's August 2015 "London Calling" report and took issue with claims about attribution.

142 Adam Segal, "Why China Hacks the World," *Christian Science Monitor*, January 31, 2016, http://www.csmonitor.com/World/Asia-Pacific/2016/0131/Why-China-hacks-the-world.

143 "Iran Loses $150 Billion a Year Due to Brain Drain," MEHR News Agency, January 8, 2014, http://en.mehrnews.com/news/101558/Iran-loses-150-billion-a-year-due-to-brain-drain.

144 Secure Works Counter Threat Unit, "ThreatGroup-4127 Targets Hillary Clinton Presidential Campaign," Secureworks.com, June 16, 2016, https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign.

145 The compromises of several certificate authorities by "ComodoHacker," the individual responsible for the DigiNotar breach, appear to have used a stolen Israeli credit card for registering domains used in the attack.

146 Office of the Press Secretary, "Executive Order: Blocking the Property and Suspending Entry Into the United States of Certain Persons With Respect to Grave Human Rights Abuses by the Governments of Iran and Syria via Information Technology," White House, news release, April 23, 2012, https://www.treasury.gov/resource-center/sanctions/Programs/Documents/2012iran_syria_eo.pdf.

147 "Sanctions Related to Significant Cyber-Enabled Malicious Activities," U.S. Department of the Treasury, last modified August 9, 2017, https://www.treasury.gov/resource-center/sanctions/Programs/pages/cyber.aspx.

148 Members of Iranian threat actors do travel to countries that the United States has successfully received extraditions from.

149 Cory Bennett, "White House Pledges Cyber Cooperation With Gulf Leaders," *Hill,* May 14, 2015, http://thehill.com/policy/cybersecurity/242162-white-house-pledges-cyber-cooperation-with-gulf-states; and Ellen Nakashima, "As Cyberwarfare Heats Up, Allies Turn to U.S. Companies for Expertise," *Washington Post*, November 22, 2012, https://www.washingtonpost.com/world/national-security/as-cyberwarfare-heats-up-allies-turn-to-us-companies-for-expertise/2012/11/22/a14f764c-192c-11e2-bd10-5ff056538b7c_story.html?utm_term=.63ff1d99cfba.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

THE CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE is a unique global network of policy research centers in Russia, China, Europe, the Middle East, India, and the United States. Our mission, dating back more than a century, is to advance the cause of peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decisionmakers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

THE CARNEGIE MIDDLE EAST PROGRAM combines in-depth local knowledge with incisive comparative analysis to examine economic, sociopolitical, and strategic interests in the Arab world. Through detailed country studies and the exploration of key cross-cutting themes, the Carnegie Middle East Program, in coordination with the Carnegie Middle East Center, provides analysis and recommendations in both English and Arabic that are deeply informed by knowledge and views from the region. The Carnegie Middle East Program has special expertise in political reform and Islamist participation in pluralistic politics throughout the region.

BEIJING BEIRUT BRUSSELS MOSCOW NEW DELHI WASHINGTON

THE GLOBAL THINK TANK

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org