RESEARCH NOTES

The Washington Institute for Near East Policy ■ No. 34 ■ July 2016

Iran's Lengthening Cyber Shadow

MICHAEL EISENSTADT

Cyber is emerging as Tehran's weapon of choice for dealing with domestic opponents and foreign adversaries. For more than a decade, the Islamic Republic has waged a relentless cyber-spying campaign against Iranian opponents of the regime. Moreover, following the discovery in 2010 of cyberattacks on its nuclear program, and the imposition of new sanctions on its oil and financial sectors in 2011 and afterward, it conducted retaliatory cyberattacks against petroleum-sector targets in Saudi Arabia and against the U.S. financial sector. Meanwhile, it dramatically ramped up cyber reconnaissance efforts against foreign officials engaged in Iran policy, particularly in the United States, and critical infrastructure in the United States and elsewhere. These events underscore the growing importance that Tehran attaches to its cyber capabilities, which are likely to assume an even greater role in the coming years.

What explains Iran's growing interest in cyber? First, it fits well with elements of its strategic culture: a preference for ambiguity, standoff, and indirection when conducting potentially high-risk activities—enabling it to better manage this risk. Second, international cyber norms remain inchoate, providing Iran with margin for maneuver in this domain. Third, Iran hopes to shape these emerging cyber norms, so that its cyber-spying and offensive cyber operations become a tolerated form of behavior, much as its use of terrorism is tolerated by many members of the international community. Iran also uses cyber to demonstrate U.S. impotence in the face of Tehran's defiance of Washington—recalling Ayatollah Ruhollah Khomeini's slogan during the 1979–80 embassy hostage crisis that "the United States cannot do a damn thing."

While nuclear technology has been around for more than half a century and is a status symbol of the old international order, cyber is cutting-edge and a harbinger of the future; it is important for Iran to demonstrate mastery of both forms of high-tech Great Power achievement. Thus, Iran's cyber activities support

Michael Eisenstadt is the Kahn Fellow and director of the Military and Security Studies Program at The Washington Institute. *The author would like to thank Yitzhak ben Israel, Patrick Clawson, Olivier Decottignies, Jason Healey, Lydia Kostopoulos, Matthew Levitt, Martin Libicki, Kevjn Lim, and Shay Shabtai for their comments on an earlier draft of this paper, and Omar Mukhlis and Louisa Keeler for their invaluable research assistance. However, all errors of fact and interpretation are the author's own.*

the regime's narrative that the Islamic Republic is an emerging scientific and technological force[1] whose cyber achievements are second only to cyber superpowers Russia, China, and the United States.[2] Indeed, Iran is blessed with world-class human capital in the science, technology, engineering, and math (STEM) disciplines.[3] Its best universities turn out large numbers of first-rate students who have repeatedly placed high in recent informatics and other STEM olympiads.[4] Its main problem is holding on to this talent; political and economic conditions at home and tempting opportunities abroad often cause graduates to seek employment overseas.[5]

Finally, in the wake of the nuclear deal between the P5+1/EU and Iran, the latter has been testing to see what kind of activities it can get away with without jeopardizing sanctions relief and foreign investment. It has continued with the covert procurement of technology for its missile and nuclear programs,[6] reckless naval posturing in the Persian Gulf,[7] provocative missile launch exercises,[8] and arms transfers to proxies and allies in Syria and Yemen[9] in violation of the spirit, if not the word, of the nuclear accord and UN Security Council Resolution 2231. Cyber may provide Iran with an additional means of asserting itself, pushing back, and intimidating others that the United States and its allies might find difficult to effectively counter.

Evolving Cyber Capabilities

Iran's current cyber capabilities can trace their origins to the patriotic nationalist "hacktivist" collectives of a decade ago, such as Ashiyane, Shabgard, and Simorgh, that regularly defaced the websites of foreign organizations and governments deemed hostile to Iran. Many members of these groups were eventually coopted by the regime (perhaps in some cases coerced), continuing their operations under the banner of the "Iranian Cyber Army."[10] Meanwhile, during this period the regime moved to rein in the country's struggling reform movement and counter what Ayatollah Khamenei calls "soft warfare"—the alleged infiltration of subversive foreign cultural influences to undermine the social cohesion and legitimacy of the Islamic Republic—by closing reformist newspapers, harassing and arresting prominent reformists and bloggers, censoring and restricting access to the Internet, and jamming foreign radio and satellite TV transmissions.[11]

The events of the 2009 Green revolution, or "sedition," as Iranian government officials call it, served as a wakeup call for the regime, due to the opposition's reported use of social media to organize anti-regime protests—although subsequent assessments tended to downplay the role of social media during the unrest.[12] In response to these events, groups like the Iranian Cyber Army increased their attacks on websites associated with the reform movement and opposition groups, while the government strengthened its existing cyber surveillance capabilities, imposed restrictions on social media—limiting its use to government officials—and intensified Internet censorship. It also doubled down on plans to create a national computer operating system based on Linux (initiated in 2012), a national email service (initiated in 2013), and a national Internet, unconnected to the World Wide Web (expected to be operational sometime after 2019), to enhance cyber security in Iran.[13]

A second shock came with the discovery of the Stuxnet virus in Iran in 2010. Reportedly created and launched by the United States and Israel in 2008, Stuxnet is believed to be the first use of an offensive cyber weapon to cause physical damage to an industrial facility—in this case, to sabotage Iran's nuclear program and obviate the need for a conventional military strike to disrupt it.[14] Stuxnet is believed to have destroyed more than a thousand centrifuges enriching uranium at Natanz, delaying Iran's nuclear program by a year or more and slowing down the rate at which Iran was able to increase enrichment during the period the virus was active.[15] The attack may have had broader operational and political impacts (e.g., disruptions caused by the hunt for those who facilitated the sabotage), but little is known about these at present. Stuxnet did not do more damage, at least in part, because the malware was designed to operate undetected, inducing centrifuge failure in a way that would be attributed to material fatigue or design flaws, and not to a cyberattack,

and because it missed the most productive cascades at Natanz.[16] Had Stuxnet not been detected as a result of an apparent flaw in its design, it would have continued imposing incremental costs and delays on the Iranian nuclear program—albeit in a way that would probably have precluded dramatic results.

Further shocks followed. In September 2011 and again in May 2012, two forms of advanced spyware, Duqu and Flame, respectively, were discovered on computer networks in Iran. While Duqu is reportedly related to Stuxnet, Flame is a different animal altogether, deemed by one cybersecurity lab as the most complex piece of malware known at the time. Both are said to be used for cyberspying and network reconnaissance. The discovery of Duqu and Flame may have indicated that Iran's enemies were planning additional disruptive or destructive attacks.[17] Flame was apparently discovered on computers in Iran's Ministry of Petroleum after the latter was hit by a cyberattack in April 2012. The ministry's website went off-line for several days, although oil and gas production and exports are not believed to have been disrupted.[18]

To better enable the Islamic Republic to deal with its cyber challenges, Supreme Leader Ali Khamenei ordered the creation of the Supreme Council of Cyberspace in March 2012, to consolidate cyber decisionmaking in a single body that answered to him. This marked a further evolution of Iran's response to the cyber challenge and demonstrated that the Supreme Leader considers cybersecurity policy a national security issue.[19]

As Iran was being targeted by foreign cyberspying efforts, it ramped up its own cyberspying operation, starting with the theft in July 2011 of Internet security certificates from the Dutch company DigiNotar, which enabled Iranian authorities to hack into the email of an estimated 300,000 Iranian Gmail users.[20]

Iran likewise initiated a global cyberspying operation that targeted individuals, government entities, and critical infrastructure in at least sixteen countries. This effort employed a number of techniques, including spear-phishing attacks to gain sensitive personal data and hack social media accounts, as well as spyware to download sensitive employee and operational data on critical infrastructure, including oil and gas companies, defense contractors, U.S. military installations, airports, major airlines and transportation networks, telecommunications and technology firms, educational institutions, health care providers, and a dam in upstate New York.[21] As part of this effort, Iran reportedly hacked the Navy Marine Corps intranet in August 2013; it took four months to expunge the unauthorized computer network exploitation tools from the network.[22] The network reconnaissance activities in particular were probably intended to have a deterrent effect on the United States and others by hinting at Iran's ability to attack critical infrastructure.

According to a published assessment by Mandiant of these early network reconnaissance activities, Iran's cyberspies relied on a small set of publicly available off-the-shelf tools, as well as custom tools compiled from code derived from other publicly available sources, to exploit vulnerabilities in public websites. The Iranian cyberspies often used the same IP addresses and domains for a year or more, increasing the likelihood of detection, and rarely tried to cover their tracks by using antiforensic techniques or by avoiding previously targeted sites, methods that suggest relatively rudimentary capabilities.[23]

In response to the attack on its own energy sector, Iran launched an attack in August 2012 on Saudi Aramco, erasing and corrupting the hard drives of 30,000 computers, although the attack is not known to have interfered with oil and gas operations. Two weeks later, Qatar's RasGas was affected by the virus; it may have been intentionally targeted, or the virus may have inadvertently migrated to its servers via the Internet.[24]

In September 2012, Iran initiated a series of distributed denial of service (DDoS) attacks, dubbed Operation Ababil, on the U.S. stock exchange and a number of major U.S. banks, which occurred in three waves into 2013. These attacks had a significant impact on online banking operations, forcing multiple banking websites temporarily off-line.[25] And Iran is reported to have unsuccessfully attempted attacks on Israeli and Saudi power grids, instead attacking decoy virtual infrastructure networks operated by a cybersecurity

firm.[26] Iran reportedly ramped down cyberattacks as nuclear negotiations with the P5+1/EU gained momentum in November 2013 with the conclusion of a framework agreement, demonstrating the degree to which these activities are centrally controlled and serve the regime's objectives.[27]

The most prominent known exception to this lull in anti-U.S. activities was the February 2014 cyberattack on the Las Vegas headquarters of billionaire Sheldon Adelson's Sands Corporation casino and hotel chain, in retaliation for a public statement by Adelson the previous October that seemed to call for a nuclear strike on Iran if it did not give up its own nuclear program.[28]

Iran, along with Hezbollah, conducted sporadic cyberattacks on Israeli critical infrastructure during this period, usually in times of tension, such as the Israel-Hamas war in summer 2014. These attacks were apparently intended to harass and send a warning to Israel; indeed, none of these attacks disrupted or damaged Israeli critical infrastructure or government operations.[29] Iran appears to be building up Hezbollah's cyber capabilities to employ the group as a cyberspace proxy, just as it has often used it as a terrorist and irregular warfare proxy. Thus, Iran has shared cyber tools and know-how with Hezbollah—and, in the past, Hamas—transferring certain capabilities within two to four years of their introduction in the Islamic Republic. Iranian officials are also known to have met with anti-American hackers in other parts of the world (e.g., Mexico), and it may seek such partnerships with other actors elsewhere to broaden its cyberwarfare options.[30]

Following the nuclear deal with the P5+1/EU in July 2015, Iran again ramped up cyberspying operations against U.S. officials, journalists, and academics engaged in Iran policy, presumably for intelligence purposes, using email and social media contact lists harvested from the computer of detained Iranian-American businessman Siamak Namazi.[31] Iran's cyber warriors appear to have more or less returned to their prenegotiations operational tempo, just as this period has seen the conviction of detained Iranian-American journalist Jason Rezaian (who was subsequently released), the arrest of Namazi and Nizar Zakka, a Lebanese information technology specialist with a U.S. residency permit, the arrest of a handful of reform-minded Iranian artists and journalists as well as more than a hundred "hackers," the closure of the messaging app Telegram for spreading "immoral content," and a dramatic rise of anti-American invective by Ayatollah Khamenei.[32]

At around this time, European authorities moved to shut down command-and-control computer servers in Britain, Germany, and the Netherlands allegedly being used by Iranian hackers with links to the Islamic Revolutionary Guard Corps (IRGC) to gather intelligence in the United States and a number of other countries regarding civilian and military officials, Iran policy, and critical infrastructure—information that would be essential for offensive cyber operations.[33]

Then, in May 2016, amid rising Iranian-Saudi tensions, hackers in Saudi Arabia and Iran launched a tit-for-tat hacker war after a Saudi hacker defaced the homepage of the Statistical Centre of Iran. In response, a group calling itself "Iran's Security Team" defaced the websites of Saudi Arabia's General Authority for Statistics and King Abdulaziz University. Subsequent attacks defaced or disabled the websites of the Saudi Commerce Ministry, and Iran's police and cyber police forces, judiciary, foreign ministry, national postal service, and culture ministry. There is no evidence that official entities in either country were involved in these attacks.[34]

Cyber Operations and Iran's National Security Concept

In the past decade, Iran's cyber toolkit has evolved from a low-tech means of lashing out at its enemies to a pillar of its national security concept. In fact, cyber may be emerging as a fourth leg of Iran's current deterrent/warfighting triad.[35] This triad currently consists of the ability to

- disrupt maritime traffic passing through the Strait of Hormuz;
- conduct unilateral and proxy terrorist attacks on several continents; and

- launch long-range missile and rocket strikes against targets throughout the region.

In addition, Iran's military intervention in Syria since 2011 on behalf of the Assad regime has demonstrated a nascent power-projection capability, consisting of a small number of Iranian advisors, as well as a "foreign legion" consisting of much larger numbers of Lebanese, Iraqi, Afghan, and Pakistani Shiite militia proxies, to do the heavy lifting and keep its own costs down.[36]

Cyber may well be emerging as the most important component of Tehran's deterrent posture because Iran cannot close the Strait of Hormuz without doing great harm to its own interests; nearly all its oil and gas exports and nearly all its imports pass through this choke point. This is a capability to be used in extremis only if Iran's ability to export oil has been crippled. Its ability to wage terrorism has, moreover, atrophied somewhat over the years, while the ability of its adversaries to disrupt terrorist operations has improved greatly since 9/11, as shown by the substantial number of foiled Hezbollah attacks on Israel in recent years and the bungled Iranian attacks on Israeli diplomatic targets in Europe and Asia in February 2012.[37] Thus, Iran's ability to consistently pull off successful terrorist attacks is in doubt. And while its missile arsenal—the backbone of its strategic deterrent—provides critical capabilities, it opens Iran up to retaliation because the origin of the missiles is easily ascertained.[38]

Cyber, however, provides Tehran with a range of options not provided by the other legs of its current deterrent/warfighting triad, and with fewer risks. Cyber can be used in peacetime, since norms have not been established that would define cyberspying or cyberattacks as acts of war that justify a military response. Likewise, cyber operations are scalable, and because of the difficulty attributing responsibility for an attack on a timely basis, and in a manner that would be convincing to Americans and foreign publics (since cyber forensics do not rely on physical evidence in the traditional sense), cyber may provide a degree of standoff for Tehran. Moreover, the inherently intangible nature of cyber will raise questions about whether a particular cyber operation or attack is the action of "rogue" elements or authorized by the regime (the same questions sometimes asked about Tehran's actions in the physical domain). Finally, cyber allows Iran to strike at adversaries and to project power globally, instantaneously, and on a sustained basis, in ways it cannot in the physical domain.

Conversely, the threat of cyberattack touches on the Islamic Republic's deepest fears. Because it came to power through revolution, survival is Tehran's foremost concern, and counterrevolution its ultimate nightmare. It believes that U.S. soft warfare—perceived efforts to "weaponize" American soft power and to inculcate foreign ideas, values, and ideologies in order to undermine the Islamic Republic, often by cyber-enabled means such as social media and the Internet—is an even greater threat to the regime's survival than a foreign military strike or invasion.[39]

Iran believes that domestic and foreign threats form a seamless web, and that the domestic opposition is inspired by foreign cultural influences and enabled by foreign powers that seek to bring down the Islamic Republic. It likewise believes that Western popular culture has a morally corrosive impact on Iranian youth, and that U.S. soft warfare aims to alienate Iran's youth from the ideology of the revolution, undermine popular support for the regime, and sap the social cohesion of the Islamic Republic. It sees both as existential threats to the Islamic Republic.[40]

Thus, for Tehran, cyber represents both an existential threat and an exceptional opportunity. Tehran believes that cyber enables its domestic opponents to organize, and its foreign enemies to undermine the regime through soft warfare. But it also provides the regime with unprecedented means to control the country's population, to defend itself from both domestic and external cyber, military, and other threats, and to strike at its enemies. This is why Tehran is investing so much effort in developing its cyber capabilities: to deter both cyber and traditional military challenges, to wage its own version of soft warfare while its proxy and conventional military forces are kept in reserve, and to be

able to strike its enemies globally, instantaneously, and on a sustained basis—something it cannot do in the physical domain.

The Strategic Logic of Iran's Cyber Operations

Iran has traditionally taken a tit-for-tat approach to actions by its adversaries, responding at a level broadly commensurate to the perceived challenge. During the Iran-Iraq War (1980–88), then Majlis speaker Akbar Hashemi Rafsanjani warned Iraq that if chemical attacks continued, Iran would "retaliate in kind to the same level."[41] And when, three years ago, Iran feared an Israeli or U.S. preventive strike against its nuclear program, Ayatollah Khamenei announced that Iran would respond to an attack "on the same level that they attack us."[42] As Iran's leadership sees it, to do anything less would be to invite further pressure and challenges ("bullying") and signal acceptance of second-class status unbefitting a revolutionary regime that sees itself as the guardian of Muslim honor.[43] (Iran, however, will sometimes eschew reprisals that could entail excessive risk; for instance, it has not responded in-kind to the Stuxnet attack.)

Thus, during the Iran-Iraq War, Iran answered attacks on its oil industry with attacks on oil tankers in the Persian Gulf. It countered air raids on Tehran with rocket and missile strikes on Iraqi cities. And, as mentioned above, it threatened to reply to Iraqi chemical warfare with chemical attacks of its own and may have launched limited chemical attacks to signal its ability to retaliate.[44] More recently, as previously noted, in response to the assassination of its nuclear scientists between 2010 and 2012, some by sticky bombs, Iran attempted the assassination of several Israeli diplomats in a series of attacks in February 2012, some using sticky bombs. And in countering sanctions on its Central Bank and cyberattacks on its oil industry, it launched cyberattacks on Saudi Aramco and on U.S. financial institutions.

Iran has repeatedly hinted, through words and action, that this logic holds in the cyber domain. Thus Tehran claimed that Stuxnet infected 30,000 computers in Iran—the same number of computers subsequently destroyed by Iranian malware in its attack on Saudi Aramco.[45] Iranian malware used in network reconnaissance activities incorporated Persian-language terms in the computer code, effectively indicating the provenance of the malware.[46] Iranian hackers, moreover, used the word "Wiper" in the code of the Shamoon malware employed in the attack on Saudi Aramco—a likely allusion to the Wiper module used in the Flame malware that previously infected Iranian computers. And Iran's choice of targets demonstrates the "measure for measure" logic of its cyber operations.

While deniability may sometimes be desirable for Iran, it is not essential, as shown by the aforementioned use of Iranian hints and Persian terms in the malware code. This may not be sloppiness; deniability may simply not be a concern for Iran in the virtual domain, just as it is not a concern in the physical domain. Indeed, Iran has not always been careful to cover its involvement in covert military and proxy operations. Naval mines sown by Iran during the latter phases of its war with Iraq bore Persian markings, while weapons Iran sent to Iraqi special groups for attacks on U.S. soldiers there bore data plates indicating the date and place of manufacture in Iran.[47] It seems Tehran did not try to obscure its role in these attacks on U.S. personnel, naval vessels, or financial interests, and may even have relished poking its thumb, virtually or physically, in America's eye.

Standoff is probably more important for Tehran. Mines, proxies, and computer malware are all indirect ways of attacking U.S. interests. Likewise, cyberspying operations and malware attacks are generally routed through servers in third countries. And cyber is an inherently ambiguous policy instrument: claims of attribution often depend on esoteric technical proofs that do not take tangible form, requiring the public to trust the claims of experts or government officials. This further enhances cyber's appeal to Iran.

As for the possibility that some of these cyber operations may be the work of rogue elements, Iran has a history of radical elements acting on their own in the physical domain to force the government's hand.

Thus, radical "students" occupied the U.S. embassy in Tehran on November 4, 1979, to undermine government efforts to reestablish normal ties with the United States. (Khomeini only provided his blessing after the fact.) The British embassy in Tehran was similarly occupied and ransacked in November 2011 by Basij paramilitary forces, with no adverse consequences for those involved. And the commander of the IRGC Navy unit that detained fifteen Royal Navy sailors and marines in the Shatt al-Arab waterway in March 2007, without apparent authorization, was lauded and decorated when the episode ended well for the Islamic Republic with the humbling of Britain.[48]

Based on these precedents from the physical world, it is not impossible that some cyberattacks emanating from Iran are the work of rogue elements, either nationalist hacktivists or individuals connected in some way with Iranian government agencies. After all, the Iranian government is believed to have used hackers for hire in the past and has co-opted many nationalist hacktivists for its own purposes, while recruiting other hackers to work directly for the state. Some coopted hacktivists may be loose guns. But it is hard to believe that, in a country that has invested such resources and effort to control cyberspace, sophisticated attacks on foreign powers can be launched by individuals without government knowledge.[49] Moreover, the sophistication, scope, and scale of Iran's recent cyber operations, and the fact that they are not for financial gain but rather to garner information that would make possible offensive cyber operations, would seem to indicate Iranian government involvement.[50] Finally, it would seem that many of these cyber operations are consistent with the broader logic guiding its foreign and defense policies, thus serving Iran's national interests.

It is also worth noting that the interval between perceived "challenge" and "response" in the physical and cyber domains is very similar; although cyber activities may move at net speed, Iranian cyber operations seem to move at the speed of the Iranian national security bureaucracy. Iran often responds to perceived attacks on a timeline that is rather prolonged by Western standards. Terrorist reprisals typically occur anywhere from one to six months after a precipitating event, most often between four and six months. And, by conducting intermittent attacks, rather than intense, focused campaigns, Iran limits the potential for escalation and thereby manages risk.

Finally, just as many of Iran's activities in the physical domain are calculated to burnish the image of the Islamic Republic and support the regime's narratives—Iran as a rising power, as a technological powerhouse on par with the Great Powers, as a country not to be trifled with, as a steadfast and dependable ally (at least compared to the United States)—so are many of its activities in the cyber domain. In particular, these enterprises have been pursued with the goal of making the United States look weak and hapless. Thus, the 2012 attacks on U.S. financial institutions were often announced beforehand by the shadowy group that claimed responsibility for them —the Cyber Fighters of Izz al-Din al-Qassam—to demonstrate to the world that there was nothing America could do in response. In many ways, the psychological and moral effects created by these actions were far more important than their physical effects, a prioritization that reflects the values and preferences embedded in the Islamic Republic's strategic culture.[51]

These values and preferences have influenced Iran's past choices of cyber targets and will influence future ones as well. Thus, the hackers behind Operation Ababil demanded that the low-budget movie *Innocence of Muslims*, posted in September 2012, be removed from the Internet, enabling them to pose as defenders of Muslim honor—even though this was really not the grievance that prompted the cyberattack. (It is interesting to note that North Korean hackers similarly demanded that Sony Pictures withdraw *The Interview* because it mocked North Korean leader Kim Jong-un.) Accordingly, future cyber targets are likely to be chosen based on their ability to enhance Iran's image, or because they mock or insult the sensibilities of the regime's leadership.

In sum, the patterns and logic defining Iran's activities in the physical domain appear to have shaped its activities in the cyber domain and can be used as a

template for understanding them. Cyber enables Iran to push back at its enemies while perhaps allowing it to manage risk more effectively than is possible in the physical world. And while forensic tools can apparently trace many of these attacks back to Iran,[52] attribution cannot always be done promptly using methods that are transparent and intuitively understood by U.S. and foreign publics, further enhancing cyber's appeal for Iran's leadership.

Military Cyber Operations

Iran is also interested in cyber for military purposes. Israel reportedly employed electronic-attack and computer-network-penetration techniques to neutralize Syrian air defenses during the airstrike on the Syrian nuclear reactor at al-Kibar in 2007.[53] While these reports were never confirmed, their existence likely spurred Iran to examine this threat and its potential applications, given that such techniques could be used in an Israeli or U.S. strike on its own nuclear program.

Iran has claimed at least one military cyber success of its own: the capture of a U.S. RQ-170 stealth drone flying over Iran in December 2011. While American sources say the drone crashed in Iran due to a system malfunction, Iranian sources claim they succeeded in taking control of the craft electronically and landing it in Iran, apparently by jamming its command-and-control downlinks and spoofing its GPS.[54]

Whatever the truth regarding the raid on al-Kibar and the loss of the RQ-170, both events show that in the arcane field of cyberwarfare, claims are difficult to assess or debunk. As a result, trumpeted cyber successes can be used to impress domestic audiences or third parties without concern that they will be disproven. And given reports that the United States had prepared a cyber campaign against Iran in the event that nuclear negotiations broke down and led to conflict,[55] Iran is almost certainly examining the military uses of cyber, perhaps to disrupt enemy missile defenses, command and control, aerial and naval unmanned systems, logistics operations (which in the United States are hosted on unclassified computer networks), or critical infrastructure.

Cyber Deterrence and Escalation Dynamics

Given the growing salience of Iran's cyber capabilities, it is increasingly important for the United States and its allies to understand how cyber deterrence and escalation dynamics work vis-a-vis Tehran, and how they might evolve in the future.

CYBER DETERRENCE. Absent universally accepted norms or laws regarding cyberspying or cyberattacks, and given America's vulnerability to cyber retaliation, Washington has been extremely cautious in responding to Iranian cyberattacks.[56] In this new and still undefined domain, the United States lacks both a strategy for dealing with cyber threats, and the ability to defend critical infrastructure against a sophisticated cyberattack. Accordingly, Washington has avoided steps that could lead to further escalation with Iran.[57]

The United States has a longstanding credibility gap vis-à-vis Iran that could further complicate cyber deterrence. Although America's success at ensuring freedom of navigation in the Gulf during the Iran-Iraq War helped deter similar challenges there in the decades since (a strong forward U.S. naval presence, a clear declaratory policy, and robust military rules of engagement also helped), its responses to the 1983 Beirut Marine barracks and 1996 Khobar Towers bombings effectively taught Tehran that it can wage proxy terrorism against the United States without risking a military response or paying an unacceptable cost. This probably led Tehran to conclude that its 2011 attempt to assassinate the Saudi ambassador in Washington DC would not entail unacceptable risk. This problem has been further exacerbated by President Barack Obama's failure to act on his August 2012 chemical weapons redline in Syria, as well as his tendency to couch threats toward Iran's nuclear program in language that conveys more ambivalence than resolve.[58] These precedents have probably convinced Tehran that if it is careful and plays its cards right, it can likewise act with relative impunity in the cyber domain.

That said, Washington can take a number of steps to bolster deterrence against Iran in the cyber domain:

- set redlines only if it is willing to enforce them
- push back against Iranian efforts to test or circumvent redlines, as failure to do so will invite additional challenges
- use subtle, implied threats that play on Iranian paranoia when direct, overt threats might cause the Islamic Republic to dig in its heels to save face
- repair its credibility gap in the physical domain by demonstrating through words and deeds that it is increasingly tolerant of risk in its dealings with Iran, in the hope of a spillover effect on the virtual domain
- indicate that it will practice deterrence by both denial and punishment to introduce uncertainty into Tehran's cost-benefit calculus[59]
- respond asymmetrically and hold vital Iranian assets at risk in the event of a conflict, making the United States a more unpredictable adversary and raising the potential cost to Iran of miscalculation
- rely not only on cyber and military means to deter Iran but also on threats to wage "soft warfare," thereby playing on Tehran's deepest fears[60]

These proposed guidelines for deterring Iran must be tested in practice, however, to determine if they will work in either physical or virtual domains.

U.S. cyber capabilities may have a critical role to play in the practice of deterrence. Paranoia, rumormongering, and conspiratorial thinking are central to politics in Iran, and the cyber domain is well suited to the dissemination of rumors about U.S. military preparations that may play on the fears and concerns of Iran's decisionmakers, thereby inducing them to act with caution. Cyber fears may also help deter Iran from someday attempting a nuclear breakout. U.S. and allied cyber operations likely helped uncover past undeclared nuclear activities in Iran, and the realization that its program has been repeatedly penetrated has clearly caused Tehran great concern. To deter it from attempting a future covert nuclear breakout, Washington should reinforce the fear of being caught cheating again. To this end, Washington should try to convince Tehran that America's cyberspying capabilities render Iran's nuclear activities transparent to the United States and its partners by publicizing details about a number of game-changing military programs that could enable penetration of closed computer networks without requiring intelligence operatives to physically introduce spyware into the systems.[61]

The nuclear deal, however, envisages the possibility that the P5+1/EU might help Iran to protect its nuclear infrastructure against sabotage (in Annex III, paragraph 10).[62] This might enable Iran to entice world-class IT consultants, firms, and state entities to help thwart cyberspying that could enable offensive cyber operations, although the employment of foreign IT specialists also entails risks. Indeed, it was a Belarus-based firm working for an Iranian state entity that discovered the Stuxnet malware. Moreover, assistance Iran received from the global IT commercial security community—either directly or through the open publication of assessments of the malware found in Iranian computer networks by analysts at firms like Symantec, Kaspersky Lab, and CrySyS Lab[63]—undoubtedly provided the Islamic Republic with invaluable insights into how the malware infecting its systems worked.[64] The nuclear deal, then, may enable Iran to more effectively counter foreign cyberspying, complicating U.S. and allied efforts to detect future Iranian covert or clandestine nuclear activities and to disrupt them by nonlethal means.

Finally, although creating a system of norms against the use of offensive cyber weapons targeting civilian infrastructure would be highly desirable,[65] such a measure would probably not have a major impact on Iran's behavior. Iran has regularly violated international norms regarding the sanctity of diplomatic missions, allowing protestors in Tehran to storm the U.S. embassy in 1979, the Saudi and Kuwaiti embassies in 1987, the Danish embassy in 2006, the British embassy in 2011, and the Saudi embassy in 2016. And it sponsored or abetted attacks on U.S. embassies in Beirut in 1983 and 1984, in Kuwait in 1983,

on Israeli embassies in Buenos Aires in 1992, and in Bangkok in 1994 and 2012.

Iran has also joined every major arms-control regime, including the Chemical Weapons Convention and the Nuclear Nonproliferation Treaty; furthermore, Ayatollah Khamenei has issued a fatwa banning the development, stockpiling, and use of nuclear weapons. Yet it is not clear that Iran is in compliance with its CWC obligations, and it has a long record of engaging in undeclared activities in violation of its International Atomic Energy Agency and NPT obligations.[66] Thus, there is little reason to believe that Iran would adhere to the kinds of cyber norms and confidence-building measures recently recommended by a group of governmental experts convened by the United Nations.[67]

Tehran, moreover, has rebuffed U.S. efforts to implement confidence- and security-building measures in the Persian Gulf, where the navies of both countries operate in close proximity, believing that to do so would further entrench an unfavorable status quo.[68] For this reason, Iran would probably reject or violate confidence-building measures that would prevent it from fully exploiting cybers's game-changing potential.

Nevertheless, such a set of norms may be useful as a means of pressuring Iran and garnering international support for efforts to sanction Iran's bad behavior. At any rate, if the international community does not create a set of cyber norms, Iran will ensure that it shapes the prevailing cyber "rules of the road" and that these will serve the Islamic Republic's interests.

The recent U.S. indictment of seven Iranian computer specialists who carried out a number of the aforementioned cyberspying operations against the U.S. financial system on behalf of the IRGC was probably intended to deter future attacks by "naming and shaming" the individuals involved. It will almost certainly have little more than symbolic value, however, given that those individuals will likely remain beyond America's reach and the indictment will probably spur Iranian counterindictments against U.S. cyber warriors in accordance with Tehran's tit-for-tat approach.[69]

CYBER ESCALATION. Because Iran is pursuing an anti–status quo policy that by its very nature entails the potential for conflict with regional and Great Powers wedded to the regional status quo, managing risk and avoiding escalation looms large in its calculations—as it does for the United States. Tehran's modus operandi—its reliance on proxies, its emphasis on ambiguity and standoff, preference for indirection and reciprocity, and tendency to temporally string out rather than bunch operations—may derive, at least in part, from a desire to manage risk and prevent inadvertent escalation.

Nonetheless, the Islamic Republic has, from time to time, acted erratically and recklessly, taking actions that entailed a heightened possibility of sparking military confrontation.[70] Thus, it

- facilitated Hezbollah's bombing of the U.S. embassy (April 1983) and the U.S. Marine and French paratrooper barracks in Beirut (October 1983);
- facilitated Hezbollah's bombing of the Israeli embassy and a Jewish community center in Buenos Aires (March 1992 and July 1994, respectively);
- assassinated Iranian Kurdish oppositionists in a Berlin restaurant, leading to a rift with the European Union (September 1992);
- oversaw Saudi Hezbollah's bombing of the U.S. military barracks (Khobar Towers) in Dhahran, Saudi Arabia (June 1996);
- seized fifteen British sailors and marines conducting maritime security operations in the Shatt al-Arab waterway and held them for more than a week (March 2007);
- plotted to assassinate the Saudi ambassador to the United States in Washington DC (March–September 2011);
- acquiesced in, and perhaps encouraged, the occupation of the British embassy in Tehran by a mob (November 2011) despite near-universal condemnation of Iran's occupation of the U.S. embassy three decades prior; and

- attempted a series of attacks on Israeli targets in February 2012, including one on its embassy in New Delhi—even though India had steadfastly resisted U.S. pressure to sanction Iran's oil sector.

Because none of these actions prompted a direct military riposte or serious retribution by any of the countries involved, Tehran may believe it can get away with occasional bouts of reckless behavior that fly in the face of international norms.

So, while the Islamic Republic's leadership has shown that it is "rational" and generally risk averse, it is also occasionally prone to rash behavior and overreach—tendencies that its broad ambitions tend to amplify. This explains, in part, why U.S. relations with Iran have always been so fraught, complicated, and unpredictable.

Cyber could reinforce the potential for miscalculation. Because cyber norms do not yet exist, the boundaries between what is acceptable and intolerable are not yet clear. Targeted countries may decide where to draw the line only in the wake of an attack, especially one that is particularly damaging. Moreover, some countries may not be able to distinguish between attacks initiated by independent hacktivists or official entities, or may blame the wrong nonstate actor or state for a cyberattack. Furthermore, in some circumstances, cyber conflicts could spill over into the physical domain, especially if parties unable to respond in kind to a truly consequential cyberattack are forced to resort to traditional military means. Much will depend on the extent of disruption or damage caused by an attack.

The existence of several coalitions—some with overlapping membership—engaged in various covert campaigns and shadow wars in several places in the Middle East increases uncertainty and risk. The involvement of so many actors—the United States, Israel, Iran (and its allies), Saudi Arabia (and its allies), Qatar, Turkey, and Egypt—operating covertly and overtly, sometimes in concert and sometimes independently, employing cyber, drone strikes, terrorism, irregular proxy warfare, and conventional means in Libya, Syria, Yemen, and elsewhere, may create a heightened potential for both misattribution and crossover from the cyber to the physical domain, with the attendant possibility of horizontal and vertical escalation.[71]

Indeed, the 2011 plot to assassinate the Saudi ambassador in Washington, the series of terrorist attacks that Iran undertook against Israeli diplomatic missions in February 2012, and Iran's attempts to shoot down U.S. drones in the Gulf in November 2012 and March 2013 are all examples of how conflicts can cross geographic arenas or warfighting domains. It remains to be seen whether cyber operations increase or decrease the likelihood of domain crossover; too few instances exist to permit broader conclusions at this time.

Conclusion

The foregoing analysis has a number of implications for how the United States deals with Iran's growing cyber capabilities. These conclusions, however, should be considered somewhat tentative given the small data set; after all, the Middle East is only a decade or so into the cyberwarfare era.

The Islamic Republic sees cyber as a means of controlling its population, defending against and waging soft warfare, gathering intelligence, deterring attacks in the cyber and physical domains, and striking enemies in order to achieve *psychological* as well as *physical* effects. The pervasive dependence of advanced economies on information and communication technologies ensures Iran will always have vulnerable targets to attack, in order to be a nuisance or impose costs. And cyber may allow it to strike globally, instantaneously, and on a sustained basis in ways not possible in the physical domain.

The United States may not be able to deter all types of Iranian cyber activities due to asymmetries in interests, vulnerabilities, and risk tolerance, although it may be possible to deter attacks against certain targets or target sets.[72] More specifically, it may not be possible to deter Iranian cyberspying—at least in part because the United States itself engages in this practice—and it may be difficult to deter nuisance and cost-imposing attacks, such as DDoS attacks. For these, effective cyber defenses may be the best solution.

Iran's cyber activities show that a third-tier cyber power can carry out significant nuisance and cost-imposing attacks, though it has not yet demonstrated an ability to conduct strategic critical-infrastructure attacks. Moreover, U.S. experience with Stuxnet demonstrates that even advanced cyber powers may face challenges achieving strategic effects, due to the complexity of the system being targeted and the law of unintended consequences.[73] This assessment, however, may not hold for all types of infrastructure targets and could change as cyber reconnaissance and attack tools become more sophisticated. Much will depend on how the cyber offense/defense balance evolves.

Iran prefers to respond in kind to cyberattacks, and if thwarted, it is not clear whether it would respond in the physical domain. U.S. cyber vulnerabilities are so ubiquitous, however, that Iran is likely to always find a way of responding in-kind, even if symbolically.

One reason the Islamic Republic finds cyber so appealing is that it seems to believe there is only a *limited* potential for spillover from the cyber to the physical domain. Conversely, the United States may be so concerned about Iran's cyber capabilities at least partly because it perceives a *significant* potential for spillover from the cyber to the physical domain. The likelihood of the latter, however, may depend on the robustness of U.S. cyber defenses, ability to respond in kind—but more forcefully (i.e., its achievement of escalation dominance)—and perceived willingness to employ conventional military means in response to a major cyberattack. Preventing such spillover may therefore depend on America's ability to convince Tehran that it will respond to a truly consequential cyberattack with conventional military strikes. *Yet the perception that the U.S. resorted to Stuxnet in order to obviate the need for conventional strikes against Iran's nuclear program may thwart realization of this goal*.

To create a credible conventional military deterrent against Iranian cyberattacks, the United States will need to close the credibility gap that has precluded effective deterrence in certain arenas in the physical domain (e.g., Iran's use of terrorism). This gap has been neither acknowledged nor addressed by recent U.S. administrations.[74]

Deterrence in cyberspace—as in physical space—needs to be tailored to the Islamic Republic's value system and the history of U.S.-Iran relations: intuitive or cookie-cutter approaches are apt to fail. Yet differences between deterrence in the cyber and physical domains must also be recognized. Deterrence in the cyber domain will likely prove more difficult, due to the challenges involved in attributing responsibility for cyberattacks on a timely basis, with a high degree of confidence, and in a manner convincing to a skeptical public and international community. Moreover, pervasive U.S. cyber vulnerabilities, deriving from the scope and scale of America's critical infrastructure, will sorely tempt countries like Iran to achieve an easy "win" against a Great Power. And while America's impressive conventional military capabilities may help deter truly consequential cyberattacks on critical infrastructure, much will depend on its ability to make military deterrent threats credible.

Given the difficulty of deterring Iranian terrorism in the physical world, where well-established norms proscribe such actions, cyber deterrence where such norms do not yet exist will likely prove even more challenging. Such efforts will likely be further complicated by the Middle East operational environment, with its web of conflicts, competing power blocs. and blurred boundaries, which may increase the potential for miscalculation, domain crossover, and escalation.

As in the physical domain, Tehran may sometimes be less concerned in the cyber domain about achieving decisive physical effects than in achieving psychological and moral (i.e., propaganda) victories. For this reason, the U.S. cyber defense strategy should have a major strategic communication component that downplays Iranian cyber achievements and emphasizes America's full-spectrum cyber capabilities and societal resilience.[75]

A major benefit Tehran hopes to derive from its cyber capabilities is to burnish its image as a rising technological power; accordingly, the United States should not magnify or exaggerate Iran's cyber capabilities: it will only be doing Tehran's work. It should

instead strike a balance between downplaying these capabilities in order to deny Tehran propaganda points and emphasizing the Iranian cyber threat only as much as is needed to support U.S. diplomacy to counter it.

Tehran's way of thinking about cyber will influence its targeting strategy; this should shape U.S. cyber defense priorities. Thus, while critical infrastructure seems to be a priority target, Iran will also focus on targets perceived as enabling U.S. soft warfare: media outlets, purveyors of popular culture, think tanks seen as hostile to Iran, universities, and government agencies believed by Tehran to be active in presumed U.S. soft-warfare efforts.

When necessary, Washington should bolster deterrence against Tehran by spreading cyber rumors that feed the fears and concerns of Iran's leaders. And it should use Tehran's concerns about U.S. cyberspying capability to convince Iran's leadership that if it attempts a covert nuclear breakout, it will get caught and pay a very high price.[76]

Finally, the United States needs to continue efforts to establish norms that proscribe cyberattacks on critical infrastructure and that ensure cyber will be used in accordance with the law of armed conflict (e.g., guided by the principles of discrimination, military necessity, and proportionality). While Iran will almost certainly violate any cyber code of conduct to which it agrees, just as it has repeatedly violated its obligations under international law by attacking embassies, engaging in terrorism, and breaking its nonproliferation commitments, the existence of such norms will provide the United States with leverage to push for sanctions if and when Iran does so. This, along with more robust cyber and military deterrence postures toward Iran, could at least help constrain the Islamic Republic's behavior in the cyber domain, thereby diminishing the utility for Tehran of this potentially game-changing capability.

Notes

1. "Universities Should Play Their Part in Shaping the New Islamic Civilization," Khamenei.ir, November 13, 2015, http://english.khamenei.ir/news/2396/Universities-Should-Play-Their-Part-in-Shaping-the-New-Islamic; "Leader's Speech in Meeting with Participants of 9th Elite Youth Conference," Khamenei.ir, October 14, 2015, http://english.khamenei.ir/news/2195/Leader-s-speech-in-meeting-with-participants-of-9th-Elite-Youth; "Leader's Speech to Young Elites," Khamenei.ir, October 6, 2010, http://english.khamenei.ir/news/1400/Leader-s-Speech-to-Young-Elites.
2. Fars News Agency, "IRGC Official: Iran Enjoys 4th Biggest Cyber Army in World," February 2, 2013, http://english2.farsnews.com/newstext.php?nn=9107141074.
3. National Science Foundation, *Science & Engineering Indicators 2016*, p 2/59–60, 2/78–79, 2/83, 2/93, 5/17, https://www.nsf.gov/statistics/2016/nsb20161/uploads/1/nsb20161.pdf; Steven Ditto, *Red Tape, Iron Nerve: The Iranian Quest for U.S. Education*, Policy Focus 133 (Washington DC: Washington Institute, 2014), 1–3, http://www.washingtoninstitute.org/uploads/Documents/pubs/PolicyFocus_133_Ditto2_1.pdf.
4. "Surprising Success of Iran's Universities," *Newsweek*, August 8, 2008, http://www.newsweek.com/surprising-success-irans-universities-87853; "Review of Iran's Achievements in International Science Olympiads," *Iran Review*, June 10, 2008, http://www.iranreview.org/content/Documents/Review_of_Iran%E2%80%99s_Achievements_in_International_Scientific_Olympiads.htm; "Iran 5th in Informatics Olympiad," IRIB World Service, September 30, 2012, http://english.irib.ir/radio-culture/sci-tech/item/148139-iran-5th-in-informatics-olympiad; "Iran Ranks 6th in Intl. Olympiad in Informatics," Mehr News Agency, August 1, 2015, http://en.mehrnews.com/news/108921/Iran-ranks-6th-in-Intl-Olympiad-in-Informatics.
5. Ditto, *Red Tape, Iron Nerve*, 18–19, http://www.washingtoninstitute.org/uploads/Documents/pubs/PolicyFocus_133_Ditto2_1.pdf.
6. Associated Press, "Germany Wary of Iran's Nuclear, Missile Procurement Efforts," *New York Times*, July 8, 2016, http://www.nytimes.com/aponline/2016/07/08/world/europe/ap-eu-germany-iran-nuclear.html?_r=0.
7. Reuters, "Iranian Revolutionary Guards Fired Rockets Near U.S. Warships in Gulf: U.S.," December 29, 2015, http://www.reuters.com/article/us-usa-iran-warship-idUSKBN0UD00H20151230.
8. Reuters, "Iran Missile Tests 'Not Consistent' with Nuclear Deal Spirit: U.N. Report," July 7, 2016, http://www.reuters.com/article/us-iran-missiles-un-idUSKCN0ZN2JV.

9. Reuters, "U.S. Navy Says it Seized Weapons from Iran Likely Bound for Houthis in Yemen," April 4, 2016, http://www.reuters.com/article/us-iran-usa-yemen-arms-idUSKCN0X12DB.

10. Farvartish Rezvaniyeh, "Pulling the Strings of the Net: Iran's Cyber Army," *Frontline*, PBS, February 26, 2010, http://www.pbs.org/wgbh/pages/frontline/tehranbureau/2010/02/pulling-the-strings-of-the-net-irans-cyber-army.html.

11. Monroe Price, "Iran and the Soft War," *International Journal of Communication*, no. 6 (2012): 2397–2415, http://ijoc.org/index.php/ijoc/article/download/1654/799. For more on the control of information in Iran, see "Iran: Freedom of the Press 2015," Freedom House, https://freedomhouse.org/report/freedom-press/2015/iran; Simurgh Aryan, Homa Aryan, and J. Alex Halderman, "Internet Censorship in Iran: A First Look," *Proceedings of the 3rd USENIX Workshop on Free and Open Communications on the Internet* (August 2013), https://www.usenix.org/system/files/conference/foci13/foci13-aryan.pdf; and Mahmood Enayat, *Satellite Jamming in Iran: A War over Airwaves, Small Media Report* (November 2012), https://smallmedia.org.uk/sites/default/files/Satellite%20Jamming.pdf.

12. Evgeny Morozov, "Iran Elections: A Twitter Revolution?" *Washington Post*, June 17, 2009, http://www.washingtonpost.com/wp-dyn/content/discussion/2009/06/17/DI2009061702232.html; Nicholas Thompson, "Before You Have That Twitter-Gasm...," *Wired*, June 17, 2009, https://www.wired.com/2009/06/iran-before-you-have-that-twitter-gasm/; Matthew Weaver, "Iran's 'Twitter Revolution' Was Exaggerated, Says Editor," *Guardian*, June 9, 2010, http://www.theguardian.com/world/2010/jun/09/iran-twitter-revolution-protests.

13. Jamileh Kadivar, "Government Surveillance and Counter-Surveillance on Social and Mobile Media: The Case of Iran (2009)," *Media/Culture Journal* 18, no. 2 (2015), https://www.researchgate.net/publication/282158546_Government_Surveillance_and_Counter-Surveillance_on_Social_and_Mobile_Media_The_Case_of_Iran_2009; "Current State of Internet Censorship in Iran," ViewDNS.info, March 23, 2012, http://viewdns.info/research/current-state-of-internet-censorship-in-iran/; Article 19, *Tightening the Net: Internet Security and Censorship in Iran, Part 1: The National Internet Project* (London: Free Word Centre: 2016), https://www.article19.org/data/files/The_National_Internet_AR_KA_final.pdf.

14. David Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Broadway Books: 2012); Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown Books: 2014); Nicolas Falliere, Liam O. Murchu, and Eric Chien, "W32.Stuxnet Dossier," Symantec Security Response (February 2011), https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf; Geoff McDonald et al., "Stuxnet 0.5: The Missing Link," Symantec Security Response (February 26, 2013), http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf; Liam O. Murchu, "Countdown to Zero Day—Did Stuxnet Escape from Natanz?" Symantec Official Blog, November 11, 2014, http://www.symantec.com/connect/blogs/countdown-zero-day-did-stuxnet-escape-natanz.

15. William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iranian Nuclear Delay," *New York Times*, January 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=0; Ivanka Barzashka, "Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme," *RUSI Journal* 158, no. 2 (2013): 48–56; and Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22 (2013): 389–94.

16. Lindsay, "Stuxnet and the Limits of Cyber Warfare," 389–97. According to this assessment, "The imperative...to remain undiscovered...placed an upper bound on the damage Stuxnet could inflict: too much and Iranians would know they were under attack. Anonymity enabled the attack, but maintaining anonymity imposed a restraint upon the attacker" (p. 392).

17. "W32.Duqu: The Precursor to the Next Stuxnet," *Symantec Security Response*, November 23, 2011, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf; sKyWIper (a.k.a. Flame a.k.a. Flamer): A Complex Malware for Targeted Attacks (Budapest: CrySyS Lab, 2012), https://www.crysys.hu/skywiper/skywiper.pdf.

18. Thomas Erdbrink, "Facing Cyberattack, Iranian Officials Disconnect Some Oil Terminals from Internet," New York Times, April 23, 2012, http://www.nytimes.com/2012/04/24/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html; Reuters, "Suspected Cyber Attack Hits Iran Oil Industry," April 23, 2012, http://www.reuters.com/article/2012/04/23/us-iran-oil-cyber-idUSBRE83M0YX20120423#PeQcZJG3JvDPBAL5.97; Ellen Messmer, "Iran's Discovery of Flame Malware Turning into Political Hot Potato,"

Network World, May 30, 2012, http://www.networkworld.com/article/2188936/malware-cybercrime/iran-s-discovery-of-flame-malware-turning-into-political-hot-potato.html.

19. Gabi Siboni and Sami Kronenfeld, "Iran and Cyberspace Warfare," *Military and Strategic Affairs* 4, no. 3 (December 2012): 83–87, http://www.inss.org.il/uploadImages/systemFiles/MASA4-3Engd_Siboni%20and%20Kronenfeld.pdf; "The Supreme Council of Cyberspace: Centralizing Internet Governance in Iran," Iran Media Program (Annenberg School for Communication, University of Pennsylvania, April 8, 2013), http://www.iranmediaresearch.org/en/blog/227/13/04/08/1323.

20. Hans Hoogstraaten et al., *Black Tulip: Report of the Investigation into the DigiNotar Certificate Authority Breach* (Delft, Netherlands: Fox-IT BV, 2012), https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2012/08/13/black-tulip-update/black-tulip-update.pdf.

21. *Rocket Kitten: A Campaign with 9 Lives* (Check Point Software Technologies, November 2015), https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf; *Thamar Reservoir: An Iranian Cyber-Attack Campaign against Targets in the Middle East* (Clearsky Cyber Security, June 2015), http://www.clearskysec.com/wp-content/uploads/2015/06/Thamar-Reservoir-public1.pdf; Frederick W. Kagan and Tommy Stiansen, *The Growing Cyberthreat from Iran: The Initial Report of Project Pistachio Harvest* (American Enterprise Institute and Norse Corporation, April 2015), http://www.pistachioharvest.com/Growing_Cyberthreat_From_Iran.pdf; *Operation Cleaver* (Cylance, December 2014), http://www.cylance.com/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf; Stephen Ward, "NEWSCASTER—An Iranian Threat inside Social Media," iSight Partners, May 28, 2014, http://www.isightpartners.com/2014/05/newscaster-iranian-threat-inside-social-media/; Nart Villeneuve et al., *Operation Saffron Rose* (FireEye, 2013), https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf; United States v. Ahmad Fathi et al., criminal indictment, U.S. District Court, Southern District of New York, March 24, 2016, https://www.justice.gov/opa/file/834996/download.

22. Siobhan Gorman and Julian E. Barnes, "Iranian Hacking to Test NSA Nominee Mike Rogers: Infiltration of Navy Computer Network More Extensive than Previously Thought," *Wall Street Journal*, February 18, 2014, http://www.wsj.com/articles/SB10001424052702304899704579389402826681452.

23. *2014 Threat Report* (Mandiant, 2014), 8–10, http://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf.

24. Christopher Bronk and Eneken Tikk-Ringas, *Hack or Attack? Shamoon and the Evolution of Cyber Conflict*, Working Paper (Rice University: Baker Institute for Public Policy, 2013), http://bakerinstitute.org/files/641/.

25. Chris Strohm and Eric Engleman, "Cyber Attacks on U.S. Banks Expose Computer Vulnerability," *Bloomberg*, September 27, 2012, http://www.bloomberg.com/news/articles/2012-09-28/cyber-attacks-on-u-s-banks-expose-computer-vulnerability; Antone Gonsalves, "Bank Attackers More Sophisticated than Typical Hacktivists, Expert Says," CSO, September 28, 2012, http://www.csoonline.com/article/2132319/malware-cybercrime/bank-attackers-more-sophisticated-than-typical-hacktivists--expert-says.html; Mark Clayton, "Cyber-War: In Deed and Desire, Iran Emerging as a Major Power," *Christian Science Monitor*, March 16, 2014, http://www.csmonitor.com/World/Passcode/2014/0316/Cyber-war-In-deed-and-desire-Iran-emerging-as-a-major-power.

26. Sam Jones, "Cyber Warfare: Iran Opens a New Front," *Financial Times*, April 27, 2016, http://www.ft.com/cms/s/0/15e1acf0-0a47-11e6-b0f1-61f222853ff3.html#axzz47QW0WWyv.

27. Damian Paletta, "NSA Chief Says Iranian Cyberattacks against U.S. Have Slowed," *Wall Street Journal*, September 16, 2015, http://www.wsj.com/articles/nsa-chief-says-iranian-cyberattacks-against-u-s-have-slowed-1441905372?alg=y.

28. Benjamin Elgin and Michael Riley, "Now at the Sands Casino: An Iranian Hacker in Every Server," Bloomberg, December 11, 2014, http://www.bloomberg.com/bw/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas; Tony Capaccio, David Lerman, and Chris Strohm, "Iran behind Cyber-Attack on Adelson's Sands Corp., Clapper Says," Bloomberg, February 26, 2015, http://www.bloomberg.com/news/articles/2015-02-26/iran-behind-cyber-attack-on-adelson-s-sands-corp-clapper-says.

29. Maayan Lubell, "Iran Ups Cyber Attacks on Israeli Computers: Netanyahu," Reuters, June 9, 2013, http://www.reuters.com/article/2013/06/09/us-israel-iran-cyber-idUSBRE95808H20130609#2wLj1T3fbzbgh36W.97; Yaakov Lappin, "Iran Attempted Large-Scale Cyber-Attack on Israel, Senior Security Source

Says," *Jerusalem Post*, August 17, 2014, http://www.jpost.com/Arab-Israeli-Conflict/Iran-attempted-large-scale-cyber-attack-on-Israel-senior-security-source-says-371339; Barbara Opall-Rome, "Israel Confirms It Was Cyber Attack Target," *Defense News*, June 24, 2015, http://www.defensenews.com/story/defense/policy-budget/cyber/2015/06/24/israel-target-for-iranian-hezbollah-cyber-attacks/29210755/.

30. Siboni and Kronenfeld, *Iran and Cyberspace Warfare*, 87–88.

31. Jay Solomon, "U.S. Detects Flurry of Iranian Hacking," *Wall Street Journal*, November 4, 2015, http://www.wsj.com/articles/u-s-detects-flurry-of-iranian-hacking-1446684754; David E. Sanger and Nicole Perlroth, "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.

32. Thomas Erdbrink, "Backlash against U.S. in Iran Seems to Gather Force after Nuclear Deal," *New York Times*, November 3, 2015, http://www.nytimes.com/2015/11/04/world/middleeast/backlash-against-us-in-iran-seems-to-gather-force-after-nuclear-deal.html; Bozorgmehr Sharafedin and Sam Wilkin, "Iran's Revolutionary Guards Target Popular Messaging App in Widening Crackdown," Reuters, November 15, 2015, http://www.reuters.com/article/2015/11/15/us-iran-rights-socialmedia-idUSKCN0T40MU20151115#2s6rSAKkkb8KdyLJ.97.

33. Eric Auchard, "Iran Cyberspy Group Hit in Coordinated European Raids," Reuters, November 9, 2015, http://www.reuters.com/article/2015/11/09/us-cybersecurity-iran-idUSKCN0SY1G920151109.

34. Shahin Azimi, "Iran-Saudi Tensions Erupt in 'Cyberwar'," BBC Monitoring, June 3, 2016, http://www.bbc.com/news/world-middle-east-36438333.

35. Michael Eisenstadt, *The Strategic Culture of the Islamic Republic of Iran: Religion, Expediency, and Soft Power in an Era of Disruptive Change*, Middle East Monographs 7 (Marine Corps University, November 2015), 7–11, http://www.washingtoninstitute.org/uploads/Documents/pubs/MESM_7_Eisenstadt.pdf.

36. Ali Alfoneh and Michael Eisenstadt, "Iranian Casualties in Syria and the Strategic Logic of Intervention," *PolicyWatch* 2585 (Washington Institute for Near East Policy, March 11, 2016), http://www.washingtoninstitute.org/policy-analysis/view/iranian-casualties-in-syria-and-the-strategic-logic-of-intervention.

37. Ibid. See also Matthew Levitt, *Hizballah and the Qods Force in Iran's Shadow War with the West*, Policy Focus 123 (Washington DC: Washington Institute, 2013), http://www.washingtoninstitute.org/uploads/Documents/pubs/PolicyFocus123.pdf.

38. Michael Eisenstadt, "Missiles and the Nuclear Negotiations with Iran," *PolicyWatch* 2450 (Washington Institute for Near East Policy, July 6, 2015), http://www.washingtoninstitute.org/policy-analysis/view/missiles-and-the-nuclear-negotiations-with-iran.

39. Thus, IRGC commander Mohammad Ali Jafari has stated on several occasions that the 2009 "sedition" against the Islamic Republic—i.e., the popular protests spearheaded by the Green Movement following that year's elections—"was much more dangerous than the (eight-year) imposed war" with Iraq. "IRGC Chief Warns of Cultural Threats," Press TV, June 9, 2010, http://edition.presstv.ir/detail/129769.html. See also the statements by Jafari in Will Fulton, "Iran News Round Up," *AEI Iran Tracker*, February 28, 2013, http://www.irantracker.org/iran-news-round-february-28-2013. For more on Iran's views on soft warfare, see Price, "Iran and the Soft War," 2397–2415, http://ijoc.org/index.php/ijoc/article/download/1654/799.

40. Karim Sadjadpour, *Reading Khamenei: The World View of Iran's Most Powerful Leader* (Washington, DC: Carnegie Endowment for International Peace, 2008), 17-19, http://carnegieendowment.org/files/sadjadpour_iran_final2.pdf; "Iran's War against Western Culture: Never Ending, Always Losing," *Frontline*, PBS, December 11, 2011, http://www.pbs.org/wgbh/pages/frontline/tehranbureau/2011/12/media-the-regimes-war-against-western-culture-never-ending-always-losing.html#ixzz3QXrlC61C.

41. Akbar Hashemi Rafsanjani, interview, Tehran Domestic Service, August 28, 1986, in FBIS Daily Report—South Asia, August 29, 1986, I-4.

42. Speech by Ali Khamenei, Imam Reza's Shrine, March 20, 2012, http://english.khamenei.ir/news/1620/Leader-s-Speech-at-Imam-Ridha-s-a-s-Shrine.

43. Eisenstadt, *The Strategic Culture of the Islamic Republic of Iran*, 19–20, http://www.washingtoninstitute.org/uploads/Documents/pubs/MESM_7_Eisenstadt.pdf.

44. Ibid.

45. Fars News Agency, "Iran Warns to Reciprocate Any Possible Israeli Cyber Attack with Firm Response," August 23, 2015, http://english.farsnews.com/newstext.aspx?nn=13940601001397.

46. Garance Burke and Jonathan Fahey, "AP Investigation: US power grid vulnerable to foreign hacks," *Seattle Times*, December 21, 2015, http://www.seattletimes.com/nation-world/

ap-investigation-us-power-grid-vulnerable-to-foreign-hacks-2/.

47. Eisenstadt, *The Strategic Culture of the Islamic Republic of Iran*, p. 16, fn. 96, http://www.washingtoninstitute.org/uploads/Documents/pubs/MESM_7_Eisenstadt.pdf.

48. Ibid., 20.

49. James Lewis, quoted in Elgin and Riley, "Now at the Sands Casino," http://www.bloomberg.com/bw/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas.

50. There is an analogy here from the physical domain. In an earlier era, some argued that Iran's terrorism was the work of rogue factions and was not authorized at the highest levels of government. But its terrorism clearly conformed to the policy objectives of the government of the day, and required a high degree of coordination across government entities and agencies, which would have been impossible without agreement within the government regarding these operations. Michael Eisenstadt, *Iranian Military Power: Capabilities and Intentions*, Policy Paper 42 (Washington DC: Washington Institute, 1996), 68–69, http://www.washingtoninstitute.org/policy-analysis/view/iranian-military-power-capabilities-and-intentions. Information revealed through the process of discovery in a number of high-profile court cases supports this conclusion. See, e.g.: D. Peterson et al. v. The Islamic Republic of Iran, Ministry of Foreign Affairs, and Ministry of Information and Security, United States District Court, District of Columbia, Docket No. CA 01-2684, March 17, 2003; Iran Human Rights Documentation Center, *Murder at Mykonos: Anatomy of a Political Assassination* (March 2007), http://www.iranhrdc.org/english/publications/reports/3150-murder-at-mykonos-anatomy-of-a-political-assassination.html; USA v. Ahmed al-Mughassil et al., indictment, U.S. District Court, Eastern District of VA, Alexandria, VA, No. 01-228-A, June 2001.

51. Eisenstadt, *The Strategic Culture of the Islamic Republic of Iran*, 3, 20–23, http://www.washingtoninstitute.org/uploads/Documents/pubs/MESM_7_Eisenstadt.pdf.

52. Stewart A. Baker, "The Attribution Revolution: Raising the Costs for Hackers and Their Customers," testimony before the Subcommittee on Crime and Terrorism, Senate Judiciary Committee, May 8, 2013, https://www.judiciary.senate.gov/imo/media/doc/5-8-13BakerTestimony.pdf.

53. David A. Fulghum and Robert Wall, "U.S. Electronic Surveillance Monitored Israeli Attack on Syria," Aviation Week & Space Technology, November 21, 2007, http://aviationweek.com/awin/us-electronic-surveillance-monitored-israeli-attack-syria; David A. Fulghum, Robert Wall, and Amy Butler, "Cyber-Combat's First Shot," *Aviation Week & Space Technology*, November 26, 2007, 28–31.

54. Scott Peterson and Payam Faramarzi, "Exclusive: Iran Hijacked U.S. Drone, Says Iranian Engineer," *Christian Science Monitor*, December 15, 2011, http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video.

55. David E. Sanger and Mark Mazzetti, "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict," *New York Times*, February 16, 2016, http://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html?_r=0.

56. The United States, its allies, and the international community are still grappling with the international legal implications of offensive cyber operations. For an attempt to apply current international and customary law to offensive cyber operations, see *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2012), https://ccdcoe.org/research.html.

57. Ellen Nakashima, "U.S. Response to Bank Cyberattacks Reflects Diplomatic Caution, Vexes Bank Industry," *Washington Post*, April 27, 2013, http://www.washingtonpost.com/world/national-security/us-response-to-bank-cyberattacks-reflects-diplomatic-caution-vexes-bank-industry/2013/04/27/4a71efe2-aea2-11e2-98ef-d1072ed3cc27_story.html; Director of National Intelligence James Clapper, "Worldwide Threat Assessment of the U.S. Intelligence Community," statement to the U.S. Senate Select Committee on Intelligence, March 12, 2013, 1–3, https://www.dni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf; National Academy of Sciences, "Terrorism and the Electric Power Delivery System," November 2012, http://sites.nationalacademies.org/xpedio/groups/depssite/documents/webpage/deps_073368.pdf.

58. For more on the U.S. credibility gap, its consequences, and how to close it, see Michael Eisenstadt, "Winning Battles, Losing Wars: Rethinking American Strategy," in *U.S. Military Engagement in the Broader Middle East*, coauthored with James F. Jeffrey, Policy Focus 143 (Washington DC: Washington Institute, 2016), 68–86, http://www.washingtoninstitute.org/uploads/Documents/pubs/PolicyFocus143_JeffreyEisen.pdf.

59. Deterrence by punishment could conceivably include the assassination of key Iranian cyber personnel. While there are reports that Iranian cyber personnel have already been assassinated, it is hard to see the United States adopting this method. Damien McElroy and Ahmad Vahdat, "Iranian Cyber Warfare Commander Shot Dead in Suspected Assassination," *Telegraph*, October 2, 2013, http://www.telegraph.co.uk/news/worldnews/middleeast/iran/10350285/Iranian-cyber-warfare-commander-shot-dead-in-suspected-assassination.html.

60. For fuller treatments of how to bolster U.S. deterrence vis-à-vis Iran, see Eisenstadt, *The Strategic Culture of the Islamic Republic of Iran*, 31–32, http://www.washingtoninstitute.org/uploads/Documents/pubs/MESM_7_Eisenstadt.pdf; Michael Eisenstadt, *Deterring an Iranian Nuclear Breakout*, Research Note 26 (Washington DC: Washington Institute, 2015), 7–14, http://www.wazshingtoninstitute.org/policy-analysis/view/deterring-an-iranian-nuclear-breakout.

61. Zachary Fryer-Biggs, "DoD Looking to 'Jump the Gap' into Adversaries' Closed Networks," *Defense News*, January 15, 2013.

62. United Nations Security Council Resolution 2231 incorporating the Joint Comprehensive Plan of Action (JCPOA), http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2231(2015).

63. See, for instance, notes 14 and 17, above.

64. Lindsay, "Stuxnet and the Limits of Cyber Warfare," 394. A bug in a version of Stuxnet led it to spread beyond the enrichment plant at Natanz, and Iran, ensuring that various versions of the malware would eventually become available to computer security researchers around the world anyway.

65. Sean Lyngaas, "NSA's Rogers Makes the Case for Cyber Norms," *FCW*, February 23, 2015, https://fcw.com/articles/2015/02/23/nsa-rogers-cyber-norms.aspx; Sydney J. Freedberg Jr., "DNI, NSA Seek Offensive Cyber Clarity; OPM Not an 'Attack'," *Breaking Defense*, September 10, 2015, http://breakingdefense.com/2015/09/clapper-rogers-seek-cyber-clarity-opm-not-an-attack/2015.

66. David Albright, "Iran's Noncompliance with Its International Atomic Energy Agency Obligations," testimony, House Subcommittee on the Middle East and North Africa, Committee on Foreign Affairs, March 24, 2015, http://docs.house.gov/meetings/FA/FA13/20150324/103097/HHRG-114-FA13-Wstate-AlbrightD-20150324.pdf; Paul K. Kerr, *Iran's Nuclear Program: Tehran's Compliance with International Obligations*, Report R40094 (Congressional Research Service, April 28, 2014), http://fas.org/sgp/crs/nuke/R40094.pdf.

67. These include recommendations that participating states should: (1) not conduct or support cyber activities that damage or impair critical infrastructure; (2) not interfere with the activities of cyber response teams of other states; (3) not knowingly allow the use of their territory for internationally wrongful cyber activities; (4) provide information and assistance to prosecute terrorist and criminal use of cyber; (5) report cyber vulnerabilities and prevent the proliferation of malicious cyber tools and techniques. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," United Nations General Assembly, A/70/174, July 22, 2015, http://washin.st/2af39YD.

68. Jay Solomon and Julian E. Barnes, "U.S. Weighs a Direct Line to Iran," *Wall Street Journal*, September 19, 2011, http://www.wsj.com/articles/SB10001424053111903374004576578990787792046; Address by Adm. Mike Mullen to the Carnegie Endowment for International Peace, September 21, 2011, http://carnegieendowment.org/2011/09/20/admiral-mike-mullen/57gg; Fars News Agency, "Iran Rejects U.S. Hotline Request," November 11, 2012, http://english2.farsnews.com/newstext.php?nn=9107118530.

69. Jason Healey, quoted in David E. Sanger, "U.S. Indicts 7 Iranians in Cyberattacks on Banks and Dam," *New York Times*, March 24, 2016, http://www.nytimes.com/2016/03/25/world/middleeast/us-indicts-iranians-in-cyberattacks-on-banks-and-a-dam.html?_r=0.

70. Eisenstadt, *The Strategic Culture of the Islamic Republic of Iran*, 4–6, http://www.washingtoninstitute.org/uploads/Documents/pubs/MESM_7_Eisenstadt.pdf

71. Michael Eisenstadt, *Not by Sanctions Alone: Using Military and Other Means to Bolster Nuclear Diplomacy with Iran*, Strategic Report 13 (Washington DC: Washington Institute, 2013), 19–30, http://www.washingtoninstitute.org/uploads/Documents/pubs/StrategicReport13_Eisenstadt2.pdf.

72. James A. Lewis, "Reconsidering Deterrence for Space and Cyberspace," in *Anti-Satellite Weapons, Deterrence and Sino-American Space Relations*, ed. Michael Krepon and Julia Thompson (Washington DC: Stimson Center, 2013), 61–79, http://www.stimson.org/images/uploads/Anti-satellite_Weapons.pdf.

73. Lindsay, "Stuxnet and the Limits of Cyber Warfare," 397, 402.

74. Eisenstadt, "Winning Battles, Losing Wars," 68–86, http://www.washingtoninstitute.org/uploads/Documents/pubs/PolicyFocus143_JeffreyEisen.pdf.

75. U.S. Department of Defense, *The Department of Defense Cyber Strategy* (April 2015), http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

76. Eisenstadt, *Deterring an Iranian Nuclear Breakout*, http://www.washingtoninstitute.org/uploads/ResearchNote26_Eisenstadt-2.pdf.

1111 19th Street NW, Suite 500 • Washington, DC 20036 • www.washingtoninstitute.org