THE GROWING CYBERTHREAT FROM IRAN

THE INITIAL REPORT OF PROJECT PISTACHIO HARVEST

FREDERICK W. KAGAN AND TOMMY STIANSEN

April 2015

AEI CRITICALTHREATS.ORG
UNDERSTANDING THE CHALLENGE. TRACKING THE THREAT.

NORSE

THE GROWING CYBERTHREAT FROM IRAN

THE INITIAL REPORT OF PROJECT PISTACHIO HARVEST

Frederick W. Kagan
and Tommy Stiansen

April 2015

AMERICAN ENTERPRISE INSTITUTE CRITICAL THREATS PROJECT
AND NORSE CORPORATION

TABLE OF CONTENTS

FIGURES

EXECUTIVE SUMMARY

Iran is emerging as a significant cyberthreat to the US and its allies. The size and sophistication of the nation's hacking capabilities have grown markedly over the last few years, and Iran has already penetrated well-defended networks in the US and Saudi Arabia and seized and destroyed sensitive data. The lifting of economic sanctions as a result of the recently announced framework for a nuclear deal with Iran will dramatically increase the resources Iran can put toward expanding its cyberattack infrastructure.

We must anticipate that the Iranian cyberthreat may well begin to grow much more rapidly. Yet we must also avoid overreacting to this threat, which is not yet unmanageable. The first requirement of developing a sound response is understanding the nature of the problem, which is the aim of this report.

Pistachio Harvest is a collaborative project between Norse Corporation and the Critical Threats Project at the American Enterprise Institute to describe Iran's footprint in cyberspace and identify important trends in Iranian cyberattacks. It draws on data from the Norse Intelligence Network, which consists of several million advanced sensors distributed around the globe. A sensor is basically a computer emulation designed to look like an actual website, email login portal, or some other kind of Internet-based system for a bank, university, power plant, electrical switching station, or other public or private computer systems that might interest a hacker. Sensors are designed to appear poorly secured, including known and zero-day vulnerabilities to lure hackers into trying to break into them. The odds of accidentally connecting to a Norse sensor are low. They do not belong to real companies or show up on search engines. Data from Norse systems combined with open-source information collected by the analysts of the Critical Threats Project have allowed us to see and outline for the first time the real nature and extent of the Iranian cyberthreat.

A particular challenge is that the Islamic Republic has two sets of information technology infrastructure—the one it is building in Iran and the one it is renting and buying in the West. Both are attacking the computer systems of America and its allies, and both are influenced to different degrees by the regime and its security services. We cannot think of the Iranian cyberfootprint as confined to Iranian soil.

That fact creates great dangers for the West, but also offers opportunities. Iranian companies, including some under international sanctions and some affiliated with the Islamic Revolutionary Guard Corps (IRGC) and global terrorist organizations like Hezbollah, are hosting websites, mail servers, and other IT systems in the United States, Canada, Germany, the United Kingdom, and elsewhere. Simply by registering and paying a fee, Iranian security services and ordinary citizens can gain access to advanced computer systems and software that the West has been trying to prevent them from getting at all. The bad news is that they are getting them anyway, and in one of the most efficient ways possible—by renting what they need from us without having to go to the trouble of building or stealing it themselves.

The good news is that Western companies own these systems. They could, if they choose, deny Iranian entities sanctioned for terrorism or human rights violations access to their systems. Western governments could—and should—develop and publish lists of such entities and the cyberinfrastructure they maintain to facilitate that effort, broken down by industry. The entities hosting these systems could deal Iran a significant blow in this way, while helping to protect themselves and their other customers from the attacks coming from Iranian-rented machines.

But the Islamic Republic is also using networks within Iran to prepare and conduct sophisticated cyberattacks. Our investigations have uncovered efforts launched by the IRGC from its own computer systems to take control of American machines using sophisticated techniques. IRGC systems hit ports with known and dangerous compromises from many different systems over months. They also scanned hundreds of US systems from a single Iranian server in a few seconds. These attacks would have been lost in normal traffic if they had not all hit Norse sensor infrastructure and thereby revealed their patterns.

Sharif University of Technology, one of Iran's premier schools, conducted similar automated searches for vulnerable US infrastructure using a different

algorithm to obfuscate its activities. A Sharif IP address would try to connect with target systems on port 445 twice within a few seconds. Then a different Sharif IP address would try to connect with a different target on the same port twice within a few seconds. All of the IP addresses were clearly owned and operated by Sharif University, but none of them hosted any public-facing systems. The pattern of attacks, once again, was visible only because so many of them hit Norse infrastructure.

The attacks from the IRGC systems and from Sharif's computers could have penetrated vulnerable systems and potentially gained complete control over them. They could have used that control to attack still other Western computers while obscuring Iran's involvement almost completely. Or they could have damaged the systems they initially penetrated, which could just as well have belonged to banks, airports, power stations, or any other critical infrastructure system as to Norse.

The Iranians are, indeed, also attempting to identify vulnerable supervisory control and automated data acquisition (SCADA) systems such as those that operate and monitor our electrical grid. Norse sensors emulating such systems were probed several times in the course of our study's timeframe. It seems clear that elements within Iran are working to build a database of vulnerable systems in the US, damage to which could cause severe harm to the US economy and citizens.

The good news in all of this is that we know that the attacks Norse detected all failed—the sensors they hit were not real systems controlling anything. The bad news is that we can be certain that these were not the only attacks and equally certain that some of the others succeeded.

It would be comforting to imagine that the recently announced nuclear framework agreement will put a stop to all of this, that a new era of détente will end this cyber arms race. There is, unfortunately, no reason to believe that that will be the case. Both the White House and Iranian leadership have repeatedly emphasized that the nuclear deal is independent of all other issues outstanding between the US and Iran. The agreement itself stipulates that US sanctions against Iran for supporting terrorism and human rights violations will remain in place. Iran's behavior in Iraq, Syria, Lebanon, Yemen, and Tehran indicates that this support and those violations will continue.

Whatever the final outcome of the nuclear negotiations, we must expect that the threat of a cyberattack from Iran will continue to grow. We may have just enough time to get ready to meet that threat.

INTRODUCTION

The framework for an agreement on Iran's nuclear program announced April 2, 2015, may significantly increase the cyberthreat the Islamic Republic poses to the US and the West. Consensus is growing in the cybersecurity community that Iran's cyberwarfare capabilities are quickly increasing.[1] The rapid lifting of sanctions promised in the agreement will create an influx of resources that will fuel the expansion of these capabilities.[2] It is imperative to understand the full extent and potential of the Iranian cyberthreat and begin developing appropriate defenses and countermeasures now.

The Norse Intelligence Network, which includes a network of sensors distributed strategically to detect malicious cyber activity around the world, has received a considerable volume of cyberattacks over the past year originating from Iranian territory. In Project Pistachio Harvest, Norse and the American Enterprise Institute's (AEI) Critical Threats Project (CTP) investigations have uncovered several instances that can be attributed with moderate confidence to the Iranian regime or individuals acting on its behalf.[3] We also found Iranian efforts to suborn Western infrastructure into attacking other Western infrastructure in a way that would (later) be extremely difficult to trace back to Iran, and we can also attribute these efforts, with moderate confidence, to individuals and institutions working on behalf of the Iranian state.

Our research indicates that the Iranians have built a large and sophisticated information technology (IT) infrastructure and a cadre of talented software developers, despite international sanctions that ban most technology transfers.[4] The sanctions relief promised in the framework agreement in exchange for Iran's ceasing nuclear research and dismantling much of its enrichment infrastructure will provide the Iranian regime with much more cash with which to expand its IT capabilities. It is not yet clear, however, exactly which sanctions would be lifted under the deal.[5] Such decisions must be informed by an understanding of the roles different Iranian entities play in the cyberwarfare realm. President Barack Obama's recent executive order establishing a new cyber sanctions program must also be used to apply pressure directly against Iranian malign cyber actors.[6] These considerations must be central to the debate over managing sanctions against Iran moving forward.

Malicious Iranian cyber activity has increased significantly over the past few years, with at least three high-profile attacks attributed to Iranians, although we cannot assess whether the regime directed them or even if the same groups or individuals conducted them:

1. Iranian hackers launched distributed denial-of-service (DDoS) attacks against JPMorgan Chase, Citibank, and Bank of America in late 2011. DDoS attacks attempt to make websites inaccessible or unusable by flooding those sites with meaningless traffic. This 2011 attack was likely a response to those banks' efforts to comply with US sanctions against Iran.[7]

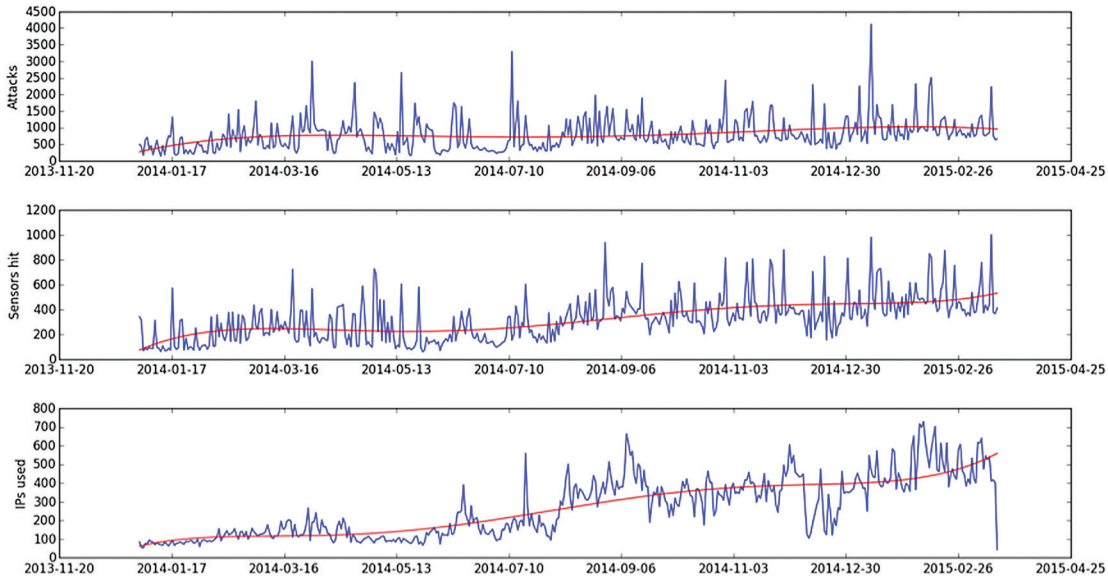
2. Iranian hackers penetrated the systems of the Las Vegas–based Sands Casino company in February 2014, effectively shutting down many of the casino's operations.[8] This attack completely wiped a significant number of Sands' hard drives and stole confidential data, posting some online. The attack was explicitly directed against Sands owner Sheldon Adelson in retaliation for remarks he made in 2013 suggesting that "Iran should be nuked."[9]

3. Iranian hackers launched malware called Shamoon against the servers of Saudi Arabia's national oil and gas company, Saudi Aramco, in August 2012. This attack destroyed significant amounts of that company's data.[10]

These attacks demonstrate Iran's evolving offensive cyber capabilities. The 2011 DDoS attacks were relatively unsophisticated affairs, albeit effective in taking US banking structure offline and causing real financial harm. Distributed denial-of-service attacks are usually launched from a network of innocent systems that hackers have (at least partially) taken over, or "compromised," in the language of cybersecurity. Such a network is called a "botnet," and each

FIGURE 1

IRANIAN CYBERINTERACTIONS WITH THE NORSE INTELLIGENCE NETWORK, JANUARY 2014–MARCH 2015



Source: Norse database.

individual computer involved in the attack is called a "bot." Today, DDoS attacks are common and are seen more as a nuisance than a real threat, although they are sometimes used as diversionary tactic to mask stealthier, more dangerous attacks. The attacks on Sands Casino and Saudi Aramco were much more sophisticated and therefore more alarming. Hackers able to conduct such attacks pose a threat to critical infrastructure systems, including the electrical grid, municipal water treatment facilities, and even nuclear reactors. Such threats to critical infrastructure are clearly a national security concern.

Data from the Norse Intelligence Network indicate that the number of cyberattacks from Iranian-controlled systems has grown significantly over the past 13 months and that these attacks have grown in sophistication, too. Attacks launched from Iranian Internet Protocol (IP) addresses increased 128 percent between January 2014 and mid-March 2015.[11] The number of individual Norse sensors hit by Iranian IPs rose 229 percent, while the number of distinct IPs used to execute these attacks rose by 508 percent (figure 1).

The Iranian cyberthreat is not yet unmanageable, but it is growing rapidly.

This last trend, shown in the bottom graph in figure 1, may be the most alarming. It suggests that hackers using Iranian IP addresses have expanded their attack infrastructure more than fivefold over the course of just 13 months. This growth greatly increases the ability of hackers in Iran to identify and compromise vulnerable systems for computer network operations (CNO), which are the use of any computer network to achieve political, financial, or military objectives. In the experience of Norse cyberanalysts, attacks generally increase in proportion to the size of the available attack

infrastructure. In other words, when an uncoordinated collection of cybercriminals take the trouble to "farm" a botnet, they tend to "harvest" its capabilities right away. It is therefore unusual and unsettling that this rule does not seem to be holding true for Iran. It could indicate that a significant portion of attacks from Iran are centrally directed and, more disturbing, that the Iranian regime might be stockpiling cyberattack capability in preparation for future contingencies.

Iran's cyberwarfare capabilities do not yet seem to rival those of Russia in skill, or of China in scale. The community of high-end hackers in Iran remains relatively small and constrained to some extent by infrastructural limitations resulting from sanctions—and the sheer difficulty of building a robust network in Iran's physical and political terrain. We have not seen evidence that Iran is capable of penetrating US national security or critical infrastructure systems outfitted with modern, best-practices cyberdefense systems.

The Iranian cyberthreat is not yet unmanageable, but it is growing rapidly. The US must rapidly develop and implement laws, sanctions, systems, and procedures to defend against this threat, lest we be surprised some day by a preventable cyber calamity.

INTELLIGENCE COLLECTION AND ANALYSIS METHODOLOGY

Project Pistachio Harvest is a unique effort that combines cyberintelligence and intelligence gathered from open (unclassified) sources about Iran to form a more complete picture of the Iranian cyber presence and threat than either discipline could provide on its own.[12] Data on cyber activities are drawn heavily from the Norse Intelligence Network collection and analysis platform, as well as from publicly available Internet registries and other tools. Open-source political, military, technical, and social intelligence about Iran is drawn from a broad array of English- and Farsi-language websites, newspapers, official outlets, and social media by analysts at the AEI Critical Threats Project.

Norse Corporation

The Norse Intelligence Network consists of several million advanced sensors distributed around the globe and operating around and within strategic data centers on millions of IP addresses in the Internet and the "Dark Web." [13] A sensor is basically a computer emulation designed to look like an actual website, email login portal, or some other kind of Internet-based system for a bank, a university, a power plant, electrical switching station, or any of a host of other sorts of public and private computer systems that might interest a hacker. Sensors are designed to appear poorly secured, including known and zero-day vulnerabilities, to lure hackers into trying to break into them. The odds of accidentally connecting to a Norse sensor are low. They do not belong to real companies or show up on search engines.

They can be somewhat fancifully compared to an opulent house with doors and windows left open while police watch from outside to see who goes in and what they try to do. The house is tucked away in a remote part of town with no passersby, no street number, no entry in any phone or address book, and no one living there. Only two kinds of people would be likely to go into it: police or others responsible for community safety, or criminals looking to loot it in some way. Occasionally some curious person might somehow find it and briefly investigate, but the honestly curious would go away quickly and either call the police or forget about it.

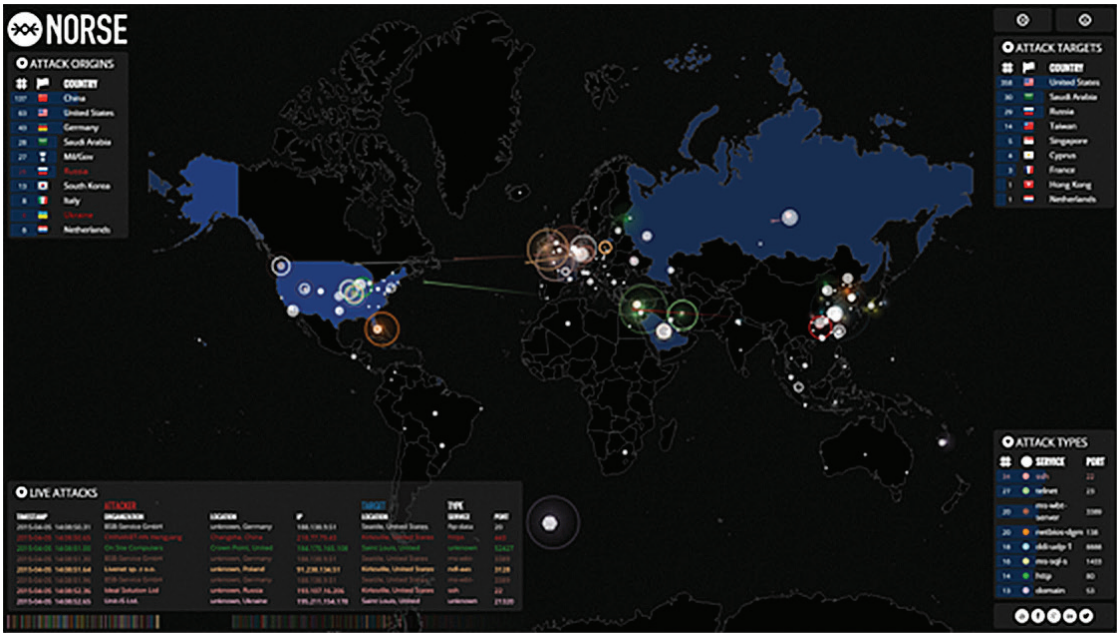
Every Internet communication must include at least six elements: the address of the originating system (source IP), the port from which the communication originated (source port), the address of the target system (destination IP), the port on the target system to which communications are directed (destination port), the date and time of the interaction, and the specific protocol used to exchange information. The Internet uses two general formats for exchanging data—Transmission Control Protocol (TCP) and the older User Datagram Protocol (UDP). One might think of them as dialects of the same data exchange language, with the caveat that ports can mean one thing in one protocol and something quite different in the other. Although many other protocols are used across the Internet, we will focus on the most common ones—IP, TCP, and UDP.

The use of ports in Internet communications is complicated, but for purposes of this report it suffices to understand a few basics. Ports are numbered from 0 to 65535 and used to indicate the particular protocol or service required for the communication. The ports below 1024 require administrator access to the system and are generally assigned to particular and well-known functions. Ports between 1024 and 49151 are called registered ports because their use for a specific purpose must in principle be approved by the International Assigned Numbers Authority, although by no means everyone abides by this requirement. Ports above 49151 can be freely assigned without registration. Examining the source and destination ports of an Internet communication, along with the protocol, can sometimes tell a cyberanalyst a great deal about the degree of control the initiator of the communication had over his system and the intended purpose of the data exchange.

Most Norse sensors sit quietly waiting for other systems to try to communicate with them. When that occurs, as seen in figure 2, the sensor records at least

FIGURE 2

NORSE LIVE ATTACK MAP DEMONSTRATES ATTACKS DETECTED AGAINST 8 MILLION SENSORS



Note: Image captured on April 5, 2015.
Source: map.ipviking.com

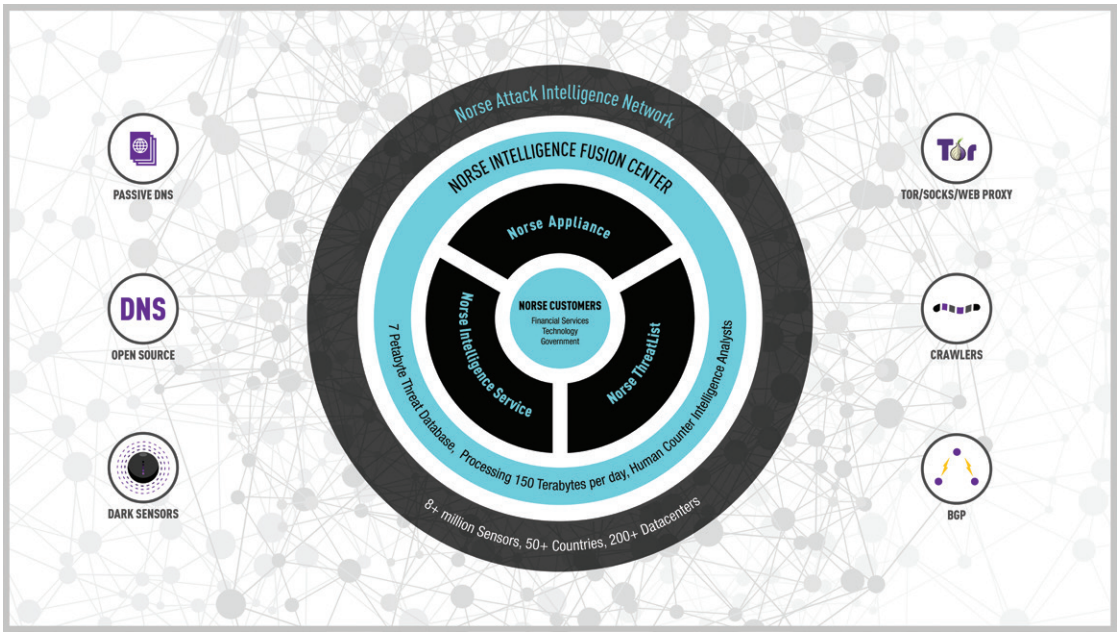
these six data points and sends them back to the main Norse database, where they are filed and analyzed. Some sensors do more than record the exchange; they actually send messages back encouraging the originator to believe that he has connected to a real computer system to get him to send even more information revealing his intentions.

Any interaction with a Norse sensor is therefore regarded as suspect. Because of the clandestine nature of the Norse infrastructure, there is no legitimate reason for anyone to attempt to communicate with any Norse sensor. Norse does not "spoof" real organizations to attempt to lure attackers. Mistakes happen, of course. People mistype addresses or inadvertently scan unintended systems, or data get otherwise misrouted. Norse therefore applies a complex formula to the interaction that takes these and many more factors into account to determine whether the intention of the originator of the interaction was innocent or malign. Malign activity, in this case, refers to connections intended to identify weaknesses in remote systems, exploit vulnerabilities to gain unauthorized access to systems or data, or prevent the system from functioning in some way. We refer to each interaction that appears to be malign as an attack.

Sensors communicate with the Norse collection infrastructure at network speed through a covert Internet structure that keeps the sensors hidden (figure 3). They are integrated with other Norse data-collection tools, including crawlers that explore the Internet looking for malicious software and indications of attacker activity. The crawlers can also be tasked dynamically to gather additional intelligence about attackers interacting with sensors, as well as the IT environment from which those attacks originate. The crawlers also report back on the kinds of operating systems their targets are using, how recently those systems have been updated or patched, and a variety of other information that helps determine whether an attacking node has itself been attacked and compromised by a third party now using the node to hit Norse infrastructure.

FIGURE 3

NORSE INTELLIGENCE NETWORK



Source: Norse Corporation

Norse systems and data thus allow for a more strategic assessment of malware campaigns than traditional cybersecurity practices, which often focus on the malware code itself and have limited visibility into the historical behavior of the Internet nodes.

In addition to the advanced data and analytics Norse provides from active cyber events, this report also uses the transparency the Internet requires to maintain its own functionality. Connecting and transporting data across the Internet appropriately requires that individuals and corporations register many components of their IT systems with a host of public and private registries. Most registries unfortunately conduct little or no verification of data provided to them, leading to a great deal of bogus information. Serious businesses and official entities, however, face market forces encouraging them to provide reasonably honest registration data. We have been able to compare and contrast registration data across multiple registries and correlate the results with crawler data and through the open-source intelligence collection efforts of the Norse and CTP analytical teams to cross-check and verify registration information in many cases.

The Critical Threats Project

AEI's Critical Threats Project has been studying Iran for five years, and has built a relational database using Palantir software (with technical and analytical support from CTP's partner, Praescient Analytics) of tens of thousands of individuals, institutions, corporations, and events associated with Iran. CTP derives its data from daily tracking of major and minor Iranian media outlets, historical data, information publicly provided by the US and other governments, and the writings of other Iran scholars.

CTP has focused particular attention on individuals and organizations connected with Iran's Islamic Revolutionary Guard Corps (IRGC), weapons of mass

destruction programs, and political environment. In partnership with the Institute for the Study of War, with which CTP shares its Palantir relational database and visualization system and works as a single analytical team, CTP has been able to monitor Iranian activities in Iraq, Syria, Lebanon, Yemen, and elsewhere around the world. This analysis enables CTP to place attack data collected by Norse into context with a deep understanding of the human and institutional shape of the Iranian regime.

Norse and CTP believe that this approach of fusing cyberintelligence with human geopolitical intelligence should become the new model for understanding cyberthreats. It opens new possibilities for thinking about responding to those threats by weighing possible real-world policy responses to online events and attacks. Iran, like all other state actors, subordinates its state-sponsored cyber activities to larger strategic and political objectives. Therefore, we must interpret observed cyber activity as operating to serve those objectives.

Norse and CTP believe that this approach of fusing cyberintelligence with human geopolitical intelligence should become the new model for understanding cyberthreats.

IRAN: THE PERFECT CYBERSTORM?

The current Iranian political, social, and economic structure is particularly well-suited to present a major cybersecurity challenge to the West for a number of reasons. Iran has a large university system that benefits from extensive state funding and is intertwined with its state security services. Its government is aggressively investing in both IT infrastructure and technical training of its people. The regime's ideology is built on anti-Americanism and the belief that the Islamic Republic is continually at war with the US, Israel, and the West. Its security doctrine defines the mere publication of views contrary to its own as an element of that war. And it has designed its national communications systems to balance popular demand for Internet access with the requirements of state control and oppression. The result is a unique accomplishment among repressive regimes: an IT infrastructure that the state can control as completely as it chooses at some times while allowing its people to interact with the rest of the world and enhance their own cyber-related skills at other times.

Supreme Leader Ayatollah Ali Khamenei has made the development of a national IT infrastructure one of the primary objectives of his economic policy. This objective is part of his effort to reduce Iran's dependence on oil exports so as to reduce the impact of potential future international sanctions. The "resistance economy" doctrine he promulgated in February 2014 directed Iran to expand "the exports share of knowledge-based products and services" and achieve "first rank" in the Middle East in this area.[14] President Hassan Rouhani announced his goal of creating 100,000 new IT jobs by 2017, while other Iranian officials claim that 20 percent of Iran's college students now pursue degrees in information technology.[15] The latter fact is the more significant because Iran is the only country in the Middle East other than Turkey and Israel to have universities ranked in the Global Top 400 by the Times Higher Education World University Rankings (2014–15): Isfahan University of Technology and Sharif University of Technology.[16]

Still, the 2014 E-Government Survey by the United Nations ranked Iran 105th overall, far below all of the Gulf Cooperation Council (GCC) states, which placed between 18th (Bahrain) and 49th (Kuwait). Iran received low scores in telecommunications infrastructure and online services, but its score for human capital was close to that of Jordan, Kuwait, and Lebanon and not too far behind the leader, Bahrain.[17]

Iran's poor infrastructure score reflects the challenges the Iranian state faces in bringing its people into the information age. Iran is far larger than any GCC state in both size and population. Its terrain is rugged and compartmentalized, and its population remains highly rural. Building and maintaining large-scale national IT infrastructure will always be much harder for Tehran than for its Arab and Turkish neighbors. The relatively high ranking of its human capital in this field, however, reflects its successful education efforts and is in some respects more important for evaluating the cyber-threat Iran might pose. A large number of talented programmers can overcome infrastructural limitations, while excellent infrastructure is useless in the hands of unskilled developers.

Technological capability is not itself a threat, of course. But the Iranian regime's belief that it is already engaged in a war with the US, Israel, Great Britain, and the West drives it to seek to control and weaponize its IT capacity as part of its doctrine known as "soft war."

Iranian leaders began speaking seriously about soft war in 2008 when they concluded that President George W. Bush was unlikely to attack Iran militarily, given the difficulties he faced in Iraq and pressures against war back home.[18] Khamenei described soft war in November 2009 as "a mixture of cultural means and advanced communication equipment to spread lies and rumors and cause doubt and divisions among the people."[19] The Iranian Armed Forces General Staff announced the establishment of a national headquarters from which to wage soft war in December 2012.[20] That announcement was followed in October 2013 with news that Iran was setting up a soft-war headquarters in each province.[21]

The Iranian military identified the Internet as one of the main enemies in this soft war, declaring, "[It is] not an instrument of threat or espionage. It's a spy itself." The head of Iran's Law Enforcement Forces in 2012 called Google an "instrument of espionage."[22]

The IRGC called for national mobilization against the Internet threat in 2014, saying, "Amid the soft war, all the society's strata, including the youths, university students and professors, should strive to confront the enemies' threats and thwart their plots." Its spokesman reported that it had developed plans "both to fight and prevent the soft war, and that all soft-power factors have been employed for an all-out confrontation with soft war."[23] This is the framework within which current Iranian cyber policy is developed and executed.

The Iranian regime's commitment to armed and unarmed struggle against the West has not been in any way diminished by the recently announced framework agreement. It is, on the contrary, hardwired into the Islamic Republic's justification for its very existence and rule. Ayatollah Ruhollah Khomeini constructed the ideology that now guides Iran by combining his own theological innovation (the "guardianship of the jurisprudent," or *velayat-e faqih*) with anti-Zionism and anti-colonialism, which rapidly evolved into explicit anti-Americanism. The current regime's efforts to expel the United States from the Middle East spring from the original anti-colonialist roots of Khomeini's ideology, which was shaped by the narrative that the US, as the inheritor of Britain's imperial power and designs, sought to dominate, oppress, and secularize the Muslim world.

The regime justifies the repression of its own people by arguing that all manifestations of anti-regime sentiment are caused by the interference of the West and/or America's determination to destroy the Islamic Republic and regain imperial control over the Middle East.[24] It justifies its military and terrorist activities as part of the "resistance to American imperial aggression, of which it sees itself as the leader. Anti-Americanism and the belief in a current and ongoing state of war between Iran and the United States are essential elements of the Islamic Republic's *raison d'état* that cannot be dispelled without fundamentally altering the character of the Iranian state.

Comparative Threats: Today's Iran versus the Historical USSR

The Iranian threat is thus somewhat different from the threat the Soviet Union posed to the US during the Cold War, despite a number of superficial similarities. Communist ideology identified capitalism as the enemy, rather than any particular capitalist state. The Soviets saw the US as the leader of the capitalist world and, therefore, a determined and dangerous enemy—but they never defined their state as opposing America specifically. The Soviet regime could thus announce that it was pursuing "peaceful coexistence" with the US, to use Nikita Khrushchev's term, or even détente, as Leonid Brezhnev said, without undermining its self-justification or weakening its self-portrayal of being perennially under siege.

The specificity of Iranian ideology, therefore, makes the prospect of real détente remote. This fact explains why Khamenei continually rejects the idea of reducing tensions with the West while simultaneously negotiating a nuclear agreement, whereas Brezhnev embraced détente during the Strategic Arms Limitation Treaty (SALT) talks in the 1970s.

It is noteworthy that the first SALT agreement in 1972 was accompanied by a statement of the "Basic Principles of Relations Between the United States of America and the Union of Soviet Socialist Republics." It began by noting the desire of both states to "strengthen peaceful relations with each other" and continued by asserting the mutual belief "that the improvement of US-Soviet relations and their mutually advantageous development in such areas as economics, science, and culture, will meet these objectives and contribute to better mutual understanding and business-like cooperation."[25] It declared, "Differences in ideology and in the social systems of the USA and the USSR are not obstacles to the bilateral development of normal relations based on the principles of sovereignty, equality, and non-interference in internal affairs and mutual advantage."

Iran's Khamenei, in contrast, has repeatedly and explicitly rejected any such broader framework for peaceful relations, reiterating on March 21, 2015: "We will by no means negotiate with the US about domestic and regional issues and the issue of arms, because American policy in the region is aimed at creating insecurity and confronting regional nations and the Islamic Awakening. That is contrary to the pivotal policies of the Islamic Republic of Iran."[26] So much for détente.

The Role of Persian Nationalism

Both Khomeini and Khamenei also welded Persian nationalism onto their ideological structure. They appeal to an interpretation of history that sees Iran as the natural hegemon of the Middle East, whose historical rights are violated whenever it is not dominant in the region. This premise flows nicely into the idea that first Britain (and then the US) were and are Iran's natural enemies, since they are responsible for depriving Iran of its rightful place of preeminence and global standing.

This element of Iran's national ideology helps explain the zeal with which younger Iranians often embrace the struggle against the US, even while partially (or completely) rejecting the theological framework of the Islamic Republic. The study of young Iranian hackers turns up individuals who praise, link to and "like" on social media liberal figures arguing for freedom of speech and expression—supporting even *Charlie Hebdo*—while simultaneously backing hacks against other Arab states and the West to protest regional maps labeling the Persian Gulf as the Arabian Gulf.

Iranian software developers and hackers have powerful incentives to play more or less by the regime's rules, even if they do not support the regime.

The degree of state control over Iran's IT infrastructure is no doubt part of the reason for the apparent willingness of Iranian developers to serve the state's needs at the expense of their own, potentially more lucrative, undertakings. The Islamic Republic has consciously designed its national IT system to give the IRGC the ability to monitor all Internet traffic in pursuit of both pornographers and political dissidents. It has worked to build a sophisticated regime of Internet censorship designed to strike a balance between keeping out "harmful" or "subversive" ideas and isolating its people to the point of creating popular resentment that could become destabilizing to the regime.

Iranian software developers and hackers thus have powerful incentives to play more or less by the regime's rules, even if they do not support the regime. It is not just that they must fear punishment if they violate those rules but also that they might benefit from the regime's investment in their IT projects by abiding by them. The regime has thus created a carrot-and-stick mechanism encouraging hackers to direct their efforts outward, allowing them to choose among nationalism, religion, or simple self-interest for their motivations as they please.

The Role of Iran's Universities

The Islamic Republic has other levers to use in encouraging its IT entrepreneurs to do its bidding. The state's role in Iran's university system is enormous, for example. The regime has invested large amounts of capital in building IT and other scientific infrastructure at its premier educational institutions—Sharif University of Technology, Shahid Beheshti University, and the IRGC-affiliated Malek Ashtar University, among others—in return for the ability to direct research in ways that further regime objectives.

The development of Iran's nuclear weapons program after 2003 offers an excellent template for understanding the evolution of the relationship between the government, security services, and universities in IT. When Khamenei ordered Iran's state-run nuclear weapons research program halted after the 2003 invasion of Iraq, his lieutenants built a new structure that federated relevant research throughout the university system.[27] The scale and ramifications of this effort are visible, but it is not easy to assess the degree to which all of the university participants in it are witting, let alone willing. Iran's IT sector functions in a similar fashion. State and security institutions "partner" with universities to conduct research that furthers state aims, making faculties and students components of regime strategic efforts. After graduation, students find themselves networked into a web of associations and research projects that tends also to support regime priorities, whether they know it or not.

The Islamic Republic also uses incentives created by mandatory military service to encourage aspiring

young programmers to support state security efforts directly. At least one scientist involved in research relevant to the development of nuclear weapons explains on his resume that he was exempted from Iran's compulsory military service in exchange for his work on a project deemed useful to the armed forces. This program of exemption was developed in 2007.[28]

Iran's leaders have thus carefully and consciously built national IT, education, and corporate infrastructures that produce excellently educated developers with incentives to pursue state objectives and avoid using their skills against the state. They have interwoven Iran's security organs, especially the IRGC, throughout these structures in ways that allow the regime to use these IT and hacking capabilities with plausible deniability. And they have constructed an Internet infrastructure designed to obfuscate the origins of malicious activity while giving the state the ability to monitor, regulate, and control citizens' access to the Internet in extremely granular ways.

Protest, Censorship, and the Iranian Internet

The massive protests after the 2009 Iranian presidential election shocked the regime. The election occurred on June 12, 2009, and protests began quickly. The protesters' use of electronic communications focused the regime's attentions on better controlling the information space. Iran had already contracted with Nokia and Siemens in 2008 to install a "monitoring center" as part of a larger contract. The regime surprised the foreign engineers who had installed the system by configuring it not only to filter traffic but also to conduct "deep packet inspection," a procedure in which monitoring software examines the content of each data packet and not just its header and routing information.[29] The use of deep packet inspection on all traffic allowed the regime to monitor its citizens to an extent the Soviets could only have dreamed of—but at the expense of slowing the Iranian Internet to a relative crawl.

Internet observer Arbor Networks reported that Iranian Internet traffic had stopped almost entirely by 6:00 p.m. Tehran time on June 13, the day after the election, and remained very low for several days. Traffic had returned to 70 percent of normal by June 16, prompting Arbor Networks to speculate that the regime turned off key national switches and routers in a rush to install new filtering systems from commercial vendors. These filtering systems did not initially have enough bandwidth to handle normal data flows, so the regime added additional "filtered bandwidth" as rapidly as it could to bring Internet traffic back to normal levels and speeds.[30]

The Iranian security services also purchased software to "filter, block and store text messages" from a Western company in 2008.[31] Among the technical requirements Iranian officials included was to "analyze all messages in English, Persian or Arabic for keywords or phrases; store them; and flag those caught by filters for review." Another was "to be able to change the content of messages." The challenge of implementing such capabilities for all Internet traffic is that the volume of that traffic is so much higher than the data generated by text messages. It is not clear how much the Iranian government succeeded in reviewing all of the Internet communications of its people, but the periodic major disruptions in Iranian Internet traffic corresponding with politically sensitive dates suggest that it made a serious effort to do so.

One such disruption in late November 2011 revealed the regime's willingness and ability to shield certain networks while slowing others to a crawl to maintain controls. Tensions between Iran and the West were running high over a detailed report by the International Atomic Energy Agency (IAEA) laying out evidence that Iran might still be pursuing nuclear weapons technology.[32] The report triggered increased Western sanctions against Iran, which in turn heightened internal Iranian tensions. Fears of an Israeli attack on Iranian nuclear facilities soared, fueled in part by an explosion at an Iranian missile base on November 13 that killed IRGC Brigadier General Hassan Tehrani Moghaddam.[33] Security services briefly arrested an adviser to President Mahmoud Ahmadinejad on November 21, and a crowd stormed the British Embassy in Tehran on November 29 in protest against the sanctions.[34] Again, the Iranian Internet virtually shut down, probably in response to these events and fears of further internal unrest.[35]

The shutdown did not affect all Iranian networks evenly, however. The major Internet networks lost upward of 90 percent of their bandwidth, but Sharif University of Technology, the University of Tehran Informatics Center, and Fanava Group all lost less than 80 percent, while Afranet and Irancell lost about 88 percent. The favored networks recovered more quickly, as well. Ten days after the throttling began, Sharif University was only 2 percent below its pre-protest norm; Afranet was down by 32 percent and Tehran University down by 47 percent, while most other networks were still down by more than 80 percent.[36] The regime's willingness to spare these providers while cutting off most of the rest of the country suggests a higher degree of confidence in these networks. That factor should be weighed in assessing the significance and possible attribution of malign traffic moving through those more "trusted" networks.

How the Regime Controls Its Internet

The regime has taken full advantage of the structure of the Internet to establish near-total control over how its people can communicate with the outside world. Internet traffic moves through a limited number of long-distance telecommunications lines into and out of a country, creating natural chokepoints at the autonomous systems (AS) that control access to them.[37]

The Iranian regime completely controls the chokepoints into and out of Iran, of which AS 12880 is by far the largest and most important, followed by AS 48159 and AS 6736.[38] The Telecommunications Infrastructure Company of Iran, a state-owned company, owns ASNs 12880 and 48159, while Iran's Research Institute for Theoretical Physics and Mathematics owns AS 6736. The regime can (technically) do almost anything with the traffic passing through these systems, including stopping, inspecting, and rerouting data packets. It can even inject its own data packets at any of these chokepoints and make it seem as if they had originated from a particular system within the Iranian network, especially if the original traffic has not been encrypted or digitally signed. The Iranian government requires all commercial Internet service providers (ISPs) to support its filtering efforts and to route international traffic through one of these state-controlled systems, making it very difficult for Iranian citizens to bypass its monitoring systems.[39]

The regime has taken full advantage of the structure of the Internet to establish near-total control over how its people can communicate with the outside world.

Attribution to the State of Iran

The Islamic Republic's commitment to determining what its people can see and what they can say (ironically) facilitates the analyst's task of attributing malicious cyber activity to the regime. In most countries, tracing malware back to a particular autonomous system or network range says little about who was actually responsible for it, because those source addresses can be faked or used as fronts by other systems. While many governments block or to varying degrees tamper with data packets that happen to move through servers located on their territory, the Iranian government is engaged in data interception and manipulation of an entirely different order.

We assert, therefore, that the typical standards of proof for attributing malicious traffic to a specific source are unnecessarily high when we examine traffic from Iranian IP addresses. It is safer than usual to say that much of the malicious traffic originating from organizations controlled or influenced by the government, or moving through networks known to be monitored and throttled by Iran's security services, is at least tacitly tolerated by the Iranian state, and in some cases, is actually sponsored by it.

We are emphatically not suggesting that *all* malicious traffic emanating from Iran is government-initiated or government-approved. Many of Iran's IT systems are outdated, unpatched, and vulnerable. This fact complicates the task of attributing intent to specific entities because so many systems in Iran are so easily suborned. Nor is the regime likely to be aware of, let

alone stop, every instance of malware moving across its wires. Attributing malware or hacking to the Iranian regime, therefore, must flow from an examination of the systems involved, the degree to which they appear compromised, and what the data flow itself can tell us about the likelihood that the originating system was an aggressor or a victim.

It is also important to note that we use the term "attribution" in an academic and policy sense, rather than a law-enforcement or military sense. We would not support using the relaxed standards of attribution we propose to target Iranian individuals or systems with military or legal response without substantial additional corroboration and evidence. The purpose of this effort is to understand what the Iranians are doing collectively and to consider possible policy or technical responses in general, rather than to identify specific perpetrators or targets for legal or military action.

WHAT ARE THE IRANIANS DOING?

The West is selling Iran IT resources with which Iran attacks Western interests. Western failures to enforce IT sanctions or to aggressively police technology transfers have allowed Iran to advance its cyber capabilities. Hundreds of thousands of domains (websites) registered to Iranian people or companies are hosted by companies in the US, Canada, and Europe. Some of those companies may actually be fronts for Iranian organizations. Others are simply companies unaware (or unconcerned) that they are doing business with Iranian entities possibly in violation of international sanctions. Norse sensors have intercepted a large volume of traffic from Iranian-controlled hosts located in the US, Canada, and other Western countries over the past several years.

The Iranian regime also uses its own domestic IT infrastructure to conduct cyber operations against the United States. Our study has traced significant volumes of malicious activity to systems controlled by the IRGC and organizations close to the Iranian government. Some of this activity targets industrial control systems, including supervisory control and data acquisition (SCADA) systems essential to running utilities and industrial automation in the West. This activity might be interpreted as an Iranian effort to establish cyber beachheads in US critical infrastructure systems—malware that is dormant for now but would allow Iran to damage or destroy those systems if it chose to do so later.

Iranian hackers have progressed far beyond website defacing or distributed denial-of-service attacks, although they boast about both. This study found evidence that they are developing sophisticated software to probe US systems for vulnerabilities, inject malware, and gain control. Their attacks are designed to blend into normal traffic and use compromised third-party systems for obfuscation. Iranian hackers are becoming a serious force in the malware world.

Iran also suffers from cyber vulnerabilities, however. International sanctions have not prevented government-affiliated and other privileged groups from purchasing advanced software, computers, and security technology, but they *have* made it very difficult for average Iranians and small-to-medium businesses to keep their systems secure. Many Iranian servers run Western software suites, some pirated or otherwise acquired informally. Unfortunately for them, pirated software is difficult to keep patched and updated. This leaves many Iranian systems riddled with relatively old, well-known, and easily exploitable vulnerabilities. As we have stipulated, this complicates the task of attributing intent to specific entities.

The prevalence of Iranian-controlled systems hosted by Western companies is problematic for several reasons. First, it likely violates international sanctions and regulations governing technology transfers to Iran. It therefore gives the Iranian state access to software, hardware, and cloud-computing services that the West had sought to withhold from Iran. It also allows Iranian individuals, companies, and security organizations to expand their cyber capabilities much more quickly and easily than they could if they had to build infrastructure in Iran. They can simply rent what they need, like any Western entity, cheaply and efficiently. Finally, it gives malign Iranian groups a degree of anonymity and legitimacy that they could not have if they were forced to operate from their own systems inside Iran. A lot of innocuous-looking traffic from Western-hosted websites is, in fact, Iranian—but discovering the connection requires painstaking effort. Understanding the nature and scope of the Iranian footprint on Western IT systems is therefore essential for assessing Iran's actual cyber capabilities.

Iran's Ashiyane Hacking Collective—Hosted in Ohio

Cybersecurity specialists have identified a handful of Iranian hacking groups and operations, but the Ashiyane hacking collective stands out for its brazenness—and for the fact that the EU sanctioned its leader for human rights violations. Ironically, it also runs a commercial cybersecurity firm, the Ashiyane Digital Security Team, in Iran that offers "ethical hacking" certificates. Its main support and discussions forum is hosted on a server in Ohio, along with a number of other websites registered in the name of its leader, Behrooz Kamalian.

FIGURE 4

ASHIYANE ANNOUNCEMENT OF DEFACING A NASA SITE

Source: www(.)zone-h(.)org

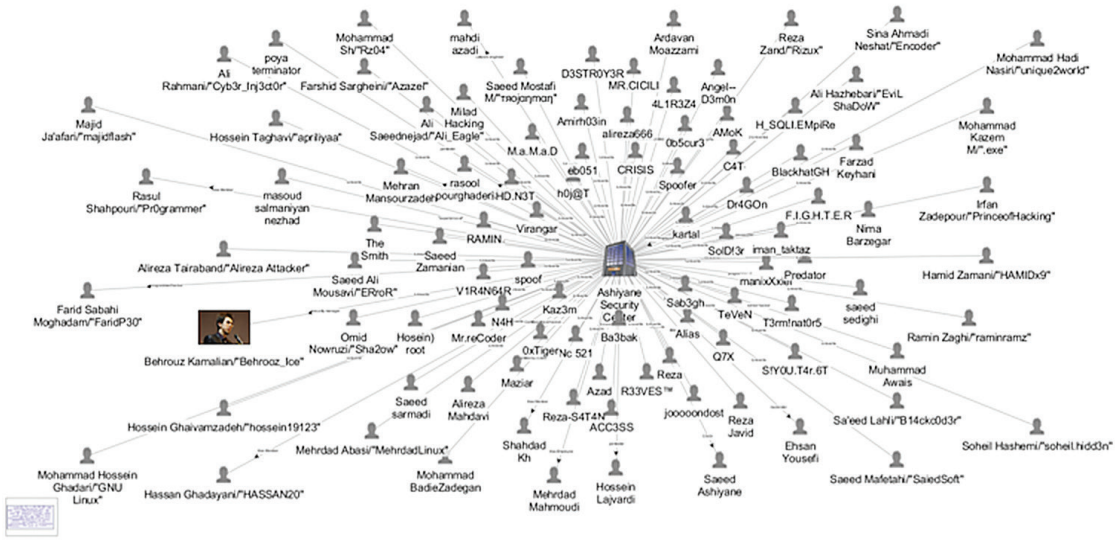
Kamalian established Ashiyane in 2002 with the ostensible goal of improving the security of Iranian websites.[40] Ashiyane seems to have started its anti-American hacking effort in 2005, in response to comments by American officials suggesting that Iran was involved in the 9/11 attacks.[41] Kamalian boasted of successful hacks against several NASA sites on Zone-h(.)org, a well-established forum on which hackers brag about defacements (figure 4). The poor English and ranting nature of these early posts speak to the relative immaturity of the hackers: "Hey Bush We Start Cybar To All American Website … wE Fuck U Bush And All American Website … All Iranian Hackers NoW Start War to uSA wEBSITE … Fuck U aND yOUR Govermenet …"(sic).

The three signatories of this post were Behrooz Kamalian (alias Behrooz-Ice), Nima Salehi (alias Q7x), and Ali Reza (alias AcTiOnSpIdEr).[42] This anti-American rant nothwithstanding, this group also attacked Iranian sites, defacing a subdomain of Sharif University of Technology in 2008 for unknown reasons.[43]

Ashiyane's pro-regime sentiments came back to the fore when Kamalian helped post pictures of anti-regime protestors in 2009, enabling Iranian police to track protesters down and arrest them. The European Union sanctioned him in 2011, stating, "'Ashiyaneh' Digital Security, founded by Behrouz Kamalian is responsible for an intensive cyber-crackdown both against domestic opponents and reformists and foreign institutions."[44] The EU designation referred to Ashiyane as an "IRGC-linked" group without offering specific evidence of the connection. An Iranian news site reporting on these designations said that Kamalian was "associated" with the IRGC, although

FIGURE 5

PUBLICLY IDENTIFIED MEMBERS OF THE ASHIYANE HACKING GROUP



Source: www(.)face2face(.)ga/index2.php and LinkedIn profiles.

it is not clear whether the site was replicating the EU report or confirming it.[45]

Ashiyane's hacking network has grown since then, and more than 40 members openly identify themselves with it (figure 5). Their ages range from about 16 to 28 years old, with the founders (now in their 30s) apparently well-established and settled enough with families that they have turned the day-to-day business of hacking over to younger coders.[46] Ashiyane has been very active, listing 65,552 defacements on Zone-h(.)org as of February 28, 2015.

Hacking is (ostensibly) a side business for Ashiyane. The group maintains a website advertising its for-profit services as an Internet security company (figure 6).[47]

No one can question the team's qualifications to conduct penetration testing of other people's servers and networks. It is more remarkable that Ashiyane actually offers fee-based training for individuals seeking Certified Ethical Hacking certificates, however.

Ethical hacking is an important component of Internet security. Ethical hackers are trained in the art of hacking but also rigorously trained in the laws, regulations, and customs governing the Internet. They commit, at least in theory, to hacking only with the knowledge and consent of the owners of target systems and for the purpose of testing security, seeking vulnerabilities, and helping the owners better protect themselves against unethical hackers.[48] Ashiyane's activities are unethical by any standard.

Yet much of Ashiyane's online infrastructure is hosted by or proxied through American companies. Ashiyane's home page, forum group, training home page, upload site, and e-magazine are proxied through CloudFlare Inc., a San Francisco company founded for the purpose of helping defend against malicious actors like Ashiyane (figure 7).[49] It is unlikely, therefore, that CloudFlare is knowingly complicit in facilitating this EU-sanctioned and IRGC-associated hacking collective. Some of Ashiyane's systems are hosted by Hetzner AG, a large German ISP, and some by XLHost, an American ISP.

Kamalian appears to maintain cyberinfrastructure in the US as well. He is listed as the registrant for 11 IP addresses and several hundred domains hosted

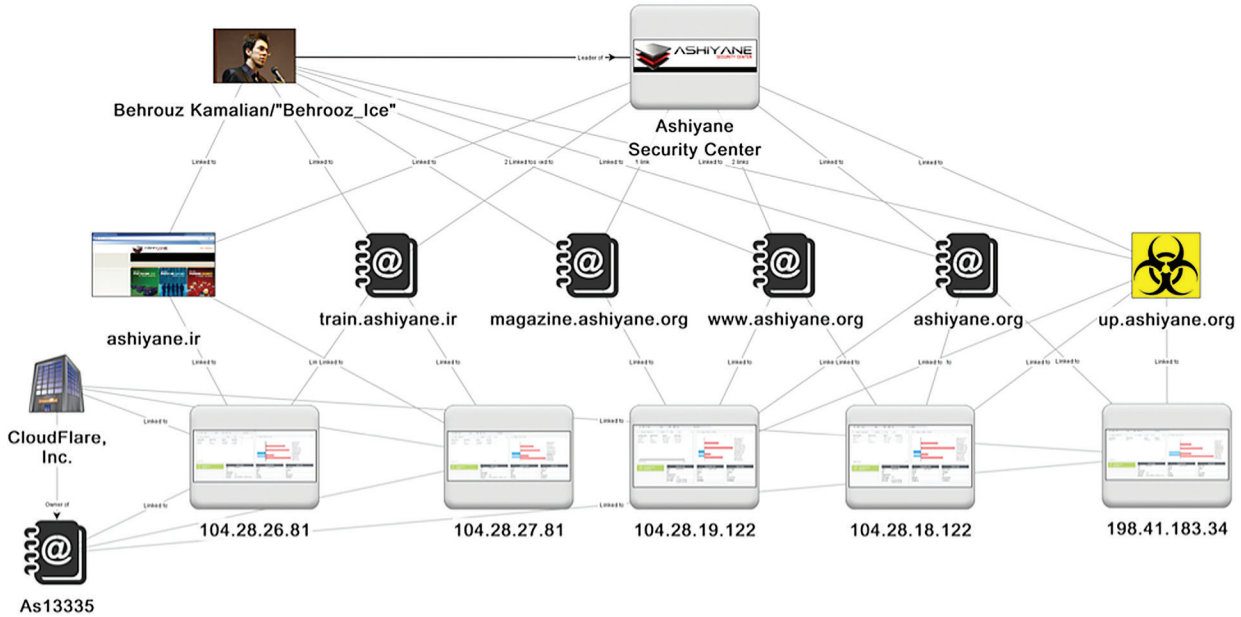
FIGURE 6

ASHIYANE HOME PAGE

Note: As of April 15, 2015.
Source: www.ashiyane(.)ir

FIGURE 7

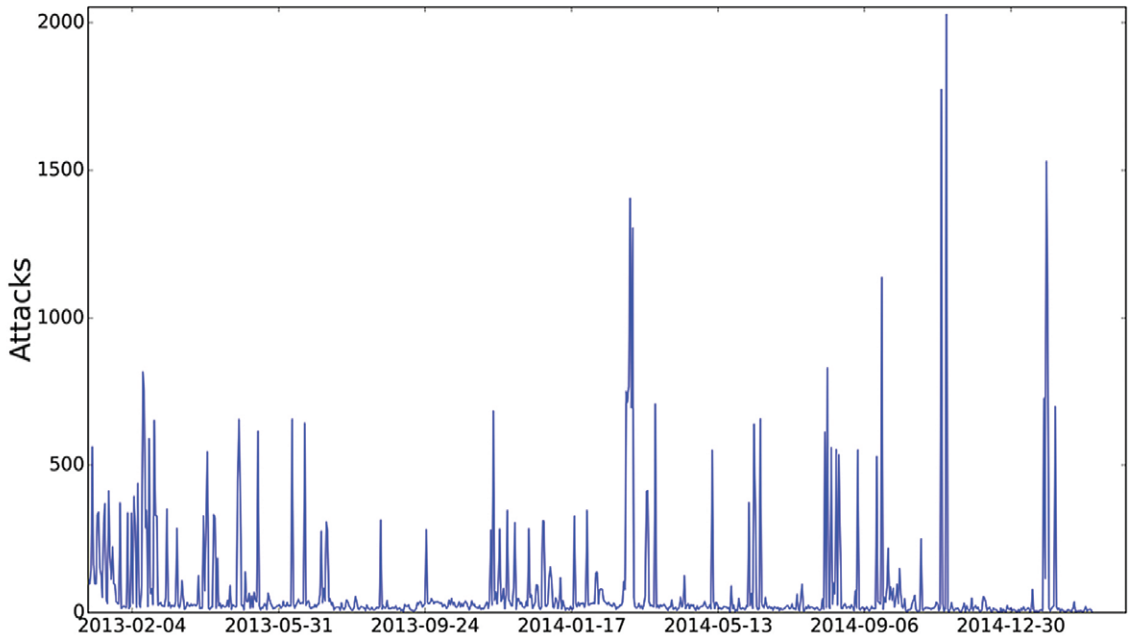
ASHIYANE IT INFRASTRUCTURE PROXIED THROUGH THE US



Note: Kamalian is the domain registrar for ashiyane(.)ir and ashiyane(.)org.
Source: Public Internet registries

FIGURE 8

CYBERATTACKS FROM XLHOST SYSTEMS AGAINST NORSE SENSORS, 2013–15



Source: Norse database.

on XLHost, giving his address in central Tehran. His IPs all have names in the form of XLHOST-BKAMALI##-#####. His address range (173.244.160.248/29) hosts a small number of domains, including some nameservers for ashiyanehost(.)com, the Farsi website of ern-co(.)com, and the domain "acount-google(.)com" (sic), which Russian cybersecurity company Kaspersky Labs and others have identified as a phishing site.[50]

XLHost: Based in Ohio, Working for Iran?

Our investigation has led us to conclude that XLHost, the company hosting Ashiyane's systems and Kamalian's IP addresses, is probably linked directly to an Iranian company willing to work on behalf of the Iranian government. XLHost identifies itself with a Tehran-based IT company, maintains a Farsi-language website, accepts Iranian currency for bill payments, and hosts multiple Hezbollah websites, in addition to the services it provides Ashiyane and Kamalian. Its systems have attacked Norse sensors tens of thousands of times over the past several years (figure 8).

The company controls about 100,000 IP addresses, some of which have attacked Norse sensors a total of at least 80,000 times over the past several years. The volume of attacks is noteworthy, but the nature of many of the attacks is more disturbing.

Thousands of the attacks originated from ports that usually require administrator access, indicating either that the owners of the system were conducting the attacks or that the systems were completely compromised by hackers.

Tens of thousands of the events involved attacks on ports relevant to accessing database and mail servers, low-level administrative systems that would provide attackers with root access, remote-access, and

other services that indicate intent to take over the target system.

A large amount of the traffic appears to have been generated by humans rather than bots because there are relatively few instances of attacks occurring within seconds of one another or of obvious "firewalking" (hitting many ports in an automated, rapid succession looking for vulnerabilities). This fact suggests that XLHost is not simply the victim of a large-scale botnet compromise.

Norse attributes 2,865 of the roughly 80,000 attack events to IPs associated with Iran over the period of October 9, 2012, through February 23, 2015.

These factors taken together suggest a concerted effort to use XLHost infrastructure to compromise US systems on a significant scale. They also suggest that some of those involved in this effort are associated with Iran in some way.

Servers physically located in the US, Canada, and Europe and owned by companies in those countries are hosting more than 40 different entities subject to US or international sanctions.

XLHost is clearly reaching out to and working on behalf of individuals in Iran. In addition to its main domain name, XLHost.com, there is also an XLHost(.)ir registered to the same address in Ohio. XLHost(.)ir is an excellent Farsi translation of the English-language XLHost site, and almost all of its links direct back to XLHost.com pages. A few of its pages are in Farsi only, however, and some of those pages indicate that payments to XLHost are accepted in Iranian rials. These facts suggest that XLHost(.)ir is simply an Iran-facing portal for XLHost itself—meaning that the company is actively soliciting business and funds from Iran for services performed in the US.

XLHost is directly furthering the interest of the Iranian regime and violating terrorism-related sanctions by hosting a website or mirror of al Manar TV, a Hezbollah-affiliated media outlet sanctioned by the US in 2006.[51] The US Department of the Treasury described al Manar as one of "the media arms of the Hezbollah terrorist network" and noted that "al Manar has employed multiple Hezbollah members. One al Manar employee engaged in preoperational surveillance for Hezbollah operations." Al Manar is known to facilitate fundraising for Hezbollah as well. [52] XLHost also hosts the Municipal Work Association website, which is a Hezbollah-affiliated site servicing populations in the Bekaa Valley and southern Lebanon, including Baalbek and Nabtiyeh.[53] The Municipal Work Association appears to be tied to the US-sanctioned Jihad al Bina (Construction Jihad) Foundation.[54]

XLHost(.)ir, furthermore, lists "Ravand Tazeh (ouriran)" in the "org" field of its registration. Ravand Tazeh is an IT company in Tehran that is associated with Ravand Cybertech operating out of Toronto, Canada. We shall consider Ravand in more detail below, but it is difficult to draw any conclusion other than that XLHost is connected with this Iran-based company and maintaining IT infrastructure in Ohio on behalf of Iranians and Lebanese Hezbollah—and which is conducting (or allowing) large-scale cyberattacks on American systems.

Western Companies Hosting Websites of Sanctioned Entities

XLHost is not alone in hosting the cyberinfrastructure of sanctioned entities. A relatively brief search, in fact, shows that servers physically located in the US, Canada, and Europe and owned by companies in those countries are hosting more than 40 different entities subject to US or international sanctions (table 1). The hosting companies range from major providers such as Germany's Hetzner AG to obscure firms that lack even rudimentary public websites.

Unless these companies are providing their services for free, they seem to be violating sanctions banning financial transactions with designated entities. They are in any case, wittingly or not, facilitating the evasion of international sanctions and providing valuable IT infrastructure to Iranian companies involved in the Iranian nuclear program.

TABLE 1

SANCTIONED ENTITIES HOSTED ON WESTERN IT SYSTEMS

URL	IP Address	Hosting Organization	Sanctioned Entity	Sanctioned By
www(.)mellatbank(.)com	75.98.174.125	A2 Hosting	Bank Mellat	US
www(.)Behzadkar(.)com	64.71.34.29	Affinity Internet	Behzadkar Co. Ltd.	Germany
www(.)tamameng(.)com	5.63.9.91	Bertina Technology Company	Tehran Tammam Engineering Services	UK
www(.)mapnablade(.)com	64.130.209.51	COMPUTOGRAM Inc.	Parto Turbine Blade Engine and Manufacturing Company	Canada, UK
www(.)farsachimie(.)com	188.40.136.5	Hetzner	Farsachimie Company	UK
www(.)fitco-ir(.)com	176.9.10.51	Hetzner	Mobin Sanjesh	EU
www(.)tavator(.)com	144.76.8.148	Hetzner	Tavator Sepahan	UK
zouchan(.)com	5.9.157.245	Hetzner	Zouchan Copper Industrial	Canada
shafapharma(.)com	88.198.60.20	Hetzner	Shifa Pharmed Industrial Group Company	Canada, Japan
www(.)eyvaztechnic(.)com	205.234.134.130	HostForWeb Inc.	Eyvaz Technic	EU, US
www(.)giecgroup(.)com	206.217.212.160	Hosting Services	GIEC	Canada
nirubattery(.)com, niruco(.)com	64.31.42.235	Limestone Networks	Niru Battery Company	UN, UK, US, EU
httsgmbh(.)de, httsgmbh(.)com	83.125.112.170	VCServer Network oHG	Hanseatic Trade Trust and Shipping (HTTS) GmbH	EU
BMIRU(.)com	78.108.80.142	Majordomo Network	Bank Melli Iran Zao	US
iranpmco(.)com	91.109.18.150	LeaseWeb	Iran Powder Metallurgy Complex	UK
Razi-center(.)net	46.165.224.58	LeaseWeb	Razi Metallurgical Research Center	UK
apadana(.)com	67.212.71.174	Netelligent Hosting Services Inc.	Kish Khodro Co Automotive Manufacturing	UK
www(.)dfsworldwide(.)com	206.188.193.46	Network Solutions	DFS Worldwide	US
parsswitch(.)com	198.178.120.118	NOC4Hosts Inc.	Pars Switch Co.	Canada
www(.)mehr-fci(.)ir	91.121.222.159	OVH	Mehr Bank	EU, US
www(.)khishavand(.)com	5.39.61.4	OVH	Schiller Novin	EU, Canada, Japan, UK
vakav-kimia(.)com, vakav(.)com	216.157.85.201	Peer 1 Dedicated Hosting	Vakav Kimia Novin	UK
www(.)landinst(.)com	78.129.202.79	Rapidswitch Ltd	Vakav Kimia Novin	UK
www(.)iran-air(.)com	72.52.4.121	Prolexic Technologies	IranAir	UK
nipc(.)net	72.52.4.91	Prolexic Technologies	National Petrochemical Company	UK, Japan

continued on the next page

TABLE 1 (CONTINUED)

URL	IP Address	Hosting Organization	Sanctioned Entity	Sanctioned By
www(.)iran-transfo(.)com	38.110.76.193	PSINet	Iran Transfo Company	EU, Canada, UK
www(.)pakshoo(.)com	38.99.139.113	PSINet	Pak Shoo Chemical and Manufacturing Company	Canada
persesanco(.)com	38.117.105.163	PSINet	Perse Sanco Ltd.	Canada, Germany
www(.)charkheshgar(.)com	198.55.50.97	Ravand Cybertech Inc.	Charkheshgar	Japan
poyeshyar(.)com	198.55.55.40	Ravand Cybertech Inc.	Poyeshar Ltd	Canada, UK
www(.)sadidpipe(.)com	198.55.50.97	Ravand Cybertech Inc.	Sadid Pipe & Profile Co.	Canada
mst-group(.)com, mst(.)ir	164.138.20.241	Ravand Tazeh	Machine Sazi Tabriz	Germany*
shomalcement(.)com	164.138.16.30	Ravand Tazeh	Shomal Cement Company	EU, Japan, US
www(.)daneshazmoon(.)com	67.228.172.101	SoftLayer Technologies Inc.	Danesh Azmoon Teb Company	Canada
spc-ir(.)com	69.56.239.13	ThePlanet.com Internet Services	Shiraz Petrochemical Company	UK
burgmann(.)com	93.184.181.65	TomCom	Burghmann-Pars (Sealing System Company)	UK
fulmen(.)com	69.195.118.88	Unified Layer	Fulmen Company	US, Switzerland, Norway, Japan, Canada, Australia, UK
ir-tc(.)com	173.254.101.29	Unified Layer	Infrared Technologists Co Ltd.	UK
www(.)parsmcs(.)com	216.158.77.100	WebNX	Pars MCS	Canada
eihbank(.)de	213.209.100.189	wilhelm.tel GmbH	Europaisch-Iranische Handelsbank AG	US

Note: *Listed as entity of concern in 2002 but not subsequently relisted.
Sources: Wisconsin Project on Nuclear Arms Control, www.iranwatch.org; US Treasury, EU, and UK designations.

Ravand Cybertech of Toronto and Tehran

In the case of Ravand Cybertech, the "Western" company hosting the systems of sanctioned Iranian companies is almost certainly the Canadian branch of an Iranian IT company. Five of the websites in table 1 are hosted by Ravand Cybertech in Canada or Ravand Tazeh in Iran, which is the same as OurIran. OurIran's website describes the company as "located in Tehran, Iran and Ontario, Canada," and adds, "We service all of Iran and the rest of the world!"[55] Amir Akhoundi Asl, technical manager at Ravand Tazeh in Tehran, also states that Ravand "has its own datacenters in Tehran and Toronto."[56] OurIran adds, "OurIran is the only hosting company in Iran which owns their own servers and have its' [sic] own private server room inside GT Data Center in Toronto Canada."[57]

Ravand's clear Iranian connections suggest why sanctioned firms might feel comfortable hosting their websites with them. At least five individuals who identify themselves on LinkedIn as Ravand Cybertech employees in Toronto have employment or education backgrounds in Iran. A senior engineer at Ravand previously worked in Tehran for an oil company, a

petroleum research institute, and the Iranian scientific network.[58] An executive director at Ravand in Canada claims to have designed the website for Shahid Beheshti University in the late 1990s.[59] Many hundreds of websites have both Ravand Cybertech and Ravand Tazeh as registration organizations.

Ravand seems to be knowingly selling advanced Internet infrastructure to entities affiliated with the Iranian state. Ravand hosts a number of Iranian banks and other commercial organizations, including in the heavily sanctioned petrochemical field.[60] Ravand Cybertech in Canada hosts more than 950 websites in the .IR domain—registration of which is controlled by the Iran Network Information Center (IRNIC), an agency of the Iranian government. IRNIC sells its domains and lists Ravand Tazeh (but not Ravand Cybertech) as an authorized reseller.[61] It is most probable either that Ravand Cybertech is receiving money to register websites and transferring it through Ravand Tazeh to IRNIC or that it is facilitating individuals' transfers of money directly to Ravand Tazeh and thence to IRNIC.

Ravand might claim that it is trying to help Iranian dissidents rather than the government, despite its clear support to government entities. It hosts Blogfa(.)ir, a very popular blogging space whose founder, Alireza Shirazi, complained in 2011 that regime censorship was damaging the Iranian blogosphere. He posted that the regime ordered him to shut down an average of 50, and sometimes as many as 10,000, blogs per week—*even though those blogs were not hosted in Iran.*[62] As long as Blogfa is obeying the orders of Iran's security organs to suppress dissident voices, it is not actually helping circumvent Iranian censorship despite the apparent desire of its founder to do so. And Ravand cannot, therefore, claim that its support for free Iranian speech on the Internet offsets the assistance it is giving the Iranian government directly.

The fact that Shirazi felt obliged to comply with the orders of the regime even though his site was not being hosted in Iran, on the contrary, highlights the dangers inherent in having Western companies host Iranian IT infrastructure. It shows that the Iranian regime believes that it can apply its laws and law enforcement to entities outside its borders and that it regards IT systems owned by Iranians abroad as subject to government control. If it can require its people to abide by its censorship regulations even on systems in Canada and against their wishes, then it may be able to require them to support more aggressive cyber activities on its behalf as well.

Iranians in the Cloud?

For Iranian companies, the wonderful new world of cloud computing offers attractive solutions to many problems. Iranian companies in the West have great access to software, hardware, and training. They can design and establish server farms with the most advanced and reliable equipment. They benefit from relatively low prices for storage, bandwidth, and electricity. The West has become a major supplier of Iran's knowledge economy despite sanctions.

Evaluating or quantifying Iranian use of cloud computing services offered by Western companies was beyond the scope of this investigation. Iranians enthusiastically avail themselves of Western web-hosting services, however, and it is reasonable to suppose that they would embrace cloud computing in a similar manner. Cloud computing is of concern because it gives Iranian interests access to vastly more computational power than they would otherwise have. They can use that power to simulate nuclear explosions; test designs for aircraft, missiles, radar, or submarines; or develop advanced encryption or decryption capabilities.

The extent of Iranian-controlled infrastructure in the West that we have already described makes the notion of actually preventing the regime from using Western cloud computing systems highly problematic. It is one thing to ask cloud computing providers not to sell to entities with .IR domains or geolocations in Iran (which are relatively straightforward to identify). But it is much harder to ask those service providers not to sell .COM, .ORG or .NET domains to Iranian entities because each registrant would have to be closely examined for connections—cyber, physical, or human—to Iranian organizations or individuals who should be denied access, a costly undertaking.

International commercial providers of cloud computing and domain hosting have not been unambiguously told not sell to Iran in any case, nor is it clear that

they would comply with such an instruction. The only feasible approach to addressing this problem would be to establish one or more organizations that maintain a database of websites and other IT systems owned by Iranian individuals, corporations, or government entities that Western law enforcement could use and then ask cloud computing providers to block or deactivate those entities on a case-by-case basis.

CYBERATTACKS DIRECTLY FROM IRAN

A considerable volume of attacks picked up by the Norse Intelligence Network originated from within the physical borders of Iran. Our investigations uncovered several instances that can be attributed with moderate confidence to the Iranian state and/or individuals acting on behalf of the Iranian regime. Furthermore, we uncovered efforts to suborn Western infrastructure into attacking other Western infrastructure in a way that would (later) be extremely difficult to trace back to Iran, and we can attribute these efforts with moderate confidence to individuals and institutions working on behalf of the Iranian state.

The sources of these attacks fall generally into three categories:

1. Many come from the large pools of IP addresses used to serve private customers in Iran. We do not consider these because attributing such attacks to particular individuals or entities is a monumental task and, in practice, impossible in most cases.

2. Others come from systems clearly owned by Iranian institutions, like universities. We have examined some of these attacks in considerable detail and concluded that we can attribute those attacks with moderate confidence to the originating institutions.

3. Still others come from servers that do not appear to belong to anyone—blocks of IP addresses registered to ISPs but lacking any websites, email servers, nameservers, or other systems typical of commercial applications. We have examined some of these and concluded that they were in fact nodes set up expressly for launching attacks and were dismantled once they were no longer needed.[63]

The rest of this paper examines the second and third categories in more detail.

Systems Clearly Owned by Iranian Institutions

The question of attribution, even in the academic sense in which we are using the term, is both grave and fraught, and it merits serious consideration. In very few cases that we have examined did Norse systems detect attacks from clearly labeled regime-controlled infrastructure or receive malware payloads that can be definitively linked to the Iranian regime or specific Iranian groups. There may well be such cases in the Norse data set, which is vast and growing, and we will continue to look for them and to make subsets of the data available in hopes that others will join in the search.

We have uncovered parts of a deliberate IRGC campaign to identify vulnerable computer systems in the US for later compromise and exploitation. They are likely parts of the first wave of a coming cyberattack.

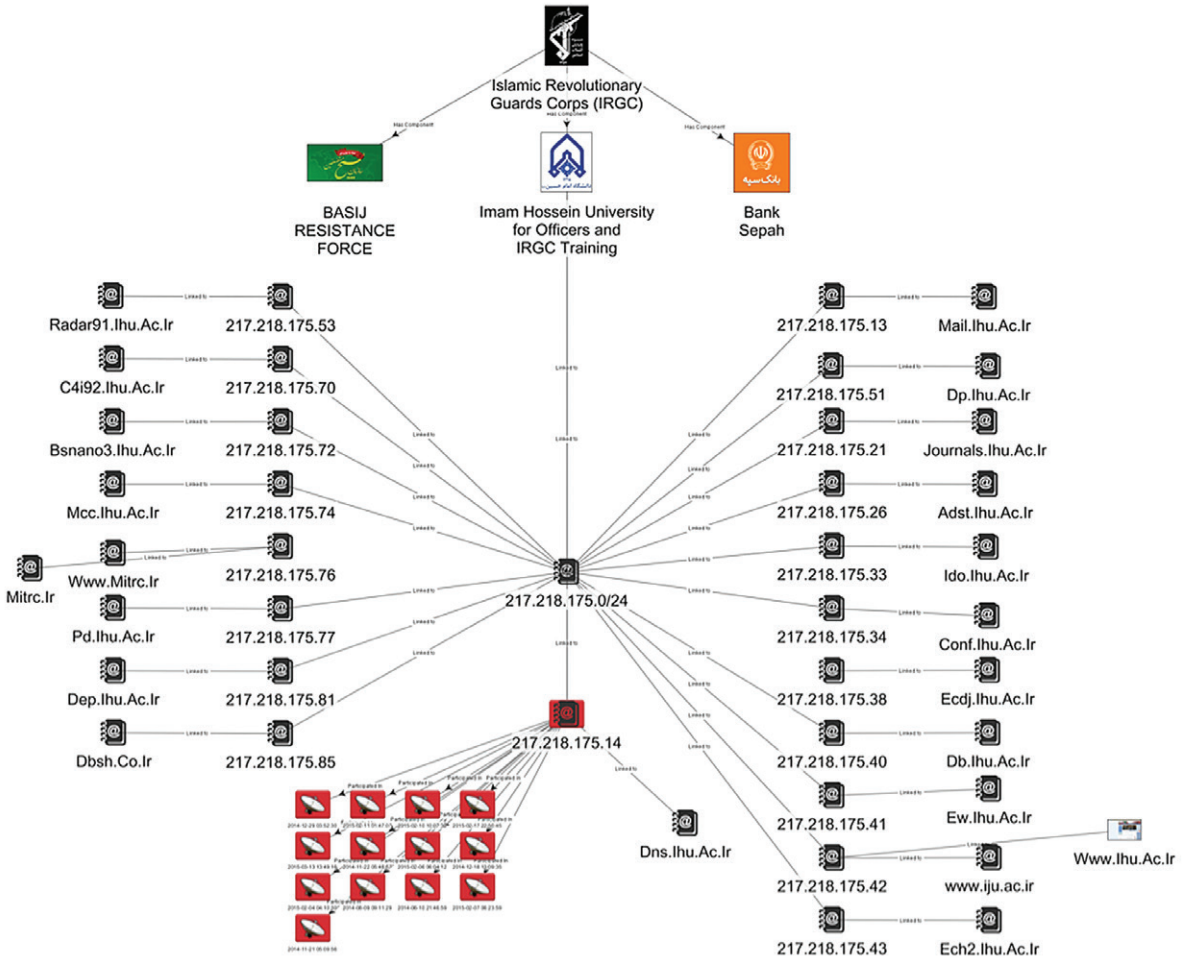
In the absence of such smoking guns, there is always room to dismiss attacks from Iranian systems as the result of poor network security, lax enforcement, or simple incompetence—and many examples of all of these surely exist. We have, therefore, focused on examples in which Iranian systems operating on networks that we either expect or know to be heavily monitored have engaged in malicious activities for more than a year.

IRGC Cyberattacks against US Systems. We believe that we have uncovered parts of a deliberate IRGC campaign to identify vulnerable computer systems in the US for later compromise and exploitation. They are likely parts of the first wave of a coming cyberattack.

The IRGC is a vast and partially clandestine enterprise. It includes a conventional military component organized into divisions and brigades, with all of the

FIGURE 9

CYBERATTACKS AND IT SYSTEMS OF IMAM HOSSEIN UNIVERSITY



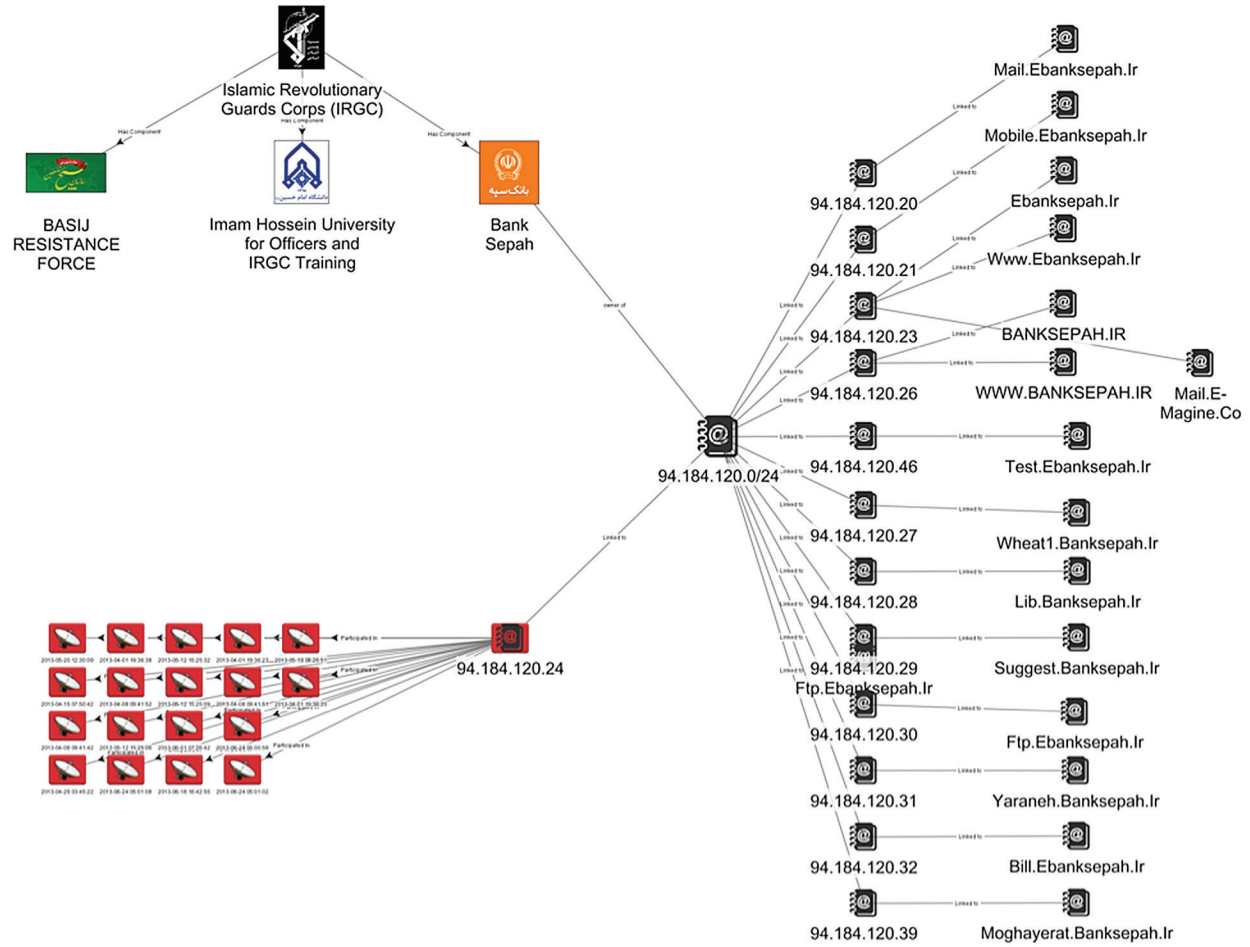
Source: Norse database.

training and support elements that any military needs. It is also an economic enterprise, owning some companies directly and others through intermediaries, especially the charitable foundations known as *bonyads* that play an outsized role in the Iranian economy. Identifying its cyberinfrastructure is therefore somewhat complicated. There is no IRGC(.)ir website (nor the appropriate Farsi equivalents), although websites do exist for the Ministry of Defense and Armed Forces Logistics, for the regular military (known as the Artesh), and for other elements of state security. The IRGC's principal charitable foundation, Bonyad Taavon Sepah, has no obvious online presence either, although some of the companies it owns do.

Other components of the IRGC, however, do maintain public websites that can be regarded as part of the IRGC cyberinfrastructure. Imam Hossein University (IHU) is the home of the IRGC's advanced military education programs—equivalent to the American war colleges and National Defense University. It controls the IP range 217.218.175.0/24, which hosts IHU's public-facing web pages, mail server, and journals page and the pages of a number of conferences IHU has hosted (figure 9). It does not host any other publicly

FIGURE 10

CYBERATTACKS AND IT SYSTEMS OF BANK SEPAH



Source: Norse database.

visible websites or servers, making it likely that IHU is the only organization with access to and control of this IP range. Malign traffic from IP addresses in this range, therefore, can be attributed to IHU with moderate confidence.

Norse sensors were attacked 13 times between June 1, 2014, and March 13, 2015, from 217.218.175.14, an IP within this range that hosts the domain nameserver for IHU.[64] All of the attacks originated on port 53, and all but one hit high ports. This is significant, as it reveals administrative-level access to the server to initiate connections from a low port. Similarly, there were no additional indicators of compromise of the IHU server. This implies the attacks did originate from the IHU server using legitimate, elevated privileges by an Iranian-based actor.

Norse sensors were also attacked 18 times between the beginning of April and the end of June 2013 from an IP belonging to Bank Sepah, the IRGC's official bank (figure 10). This IP (94.184.120.24) also had no web-facing function, but the other IPs in this subnetwork (94.184.120.0/24) hosted only systems belonging

to Bank Sepah, including its home page, mail server, mobile server, and billing server, with one exception.[65] Both the Bank Sepah and IHU IP ranges were observed attacking Norse honeypots on TCP/3389; a port used by Microsoft Remote Desktop Protocol (RDP) and leveraged by cyber actors to gain remote access to poorly secured Windows servers. This modus operandi has not been previously reported as being used by Iranian cyber actors, although it has been a staple of other state-based groups, such as Chinese hackers.[66]

IP infrastructure belonging to the Basij Resistance Force of the IRGC has conducted attacks against Norse sensors on a much larger scale than that of IHU and Sepah Bank. Ayatollah Khomeini created the Basij in 1979 as part of an effort to mobilize the Iranian people around the revolution and its defense.[67] The Basij provided much of the manpower used in the "human wave" attacks directed by the IRGC during the Iran-Iraq War and retains the role of a partially trained militia to be called up in the event of a war of national mobilization. The wars in Syria and Iraq have, in fact, drawn Basijis outside of Iran's borders, with several members publicly identified as having died in those conflicts.[68] The Basij was formally incorporated into the command structure of the IRGC in 2007 and 2008, coming under the direct control of the commander of the IRGC, currently Major General Mohammad Ali Jaafari.[69] Basijis were used in the suppression of protests after the 2009 election, which helped earn them a US Treasury Department sanctions designation for human rights violations in June 2011.[70]

The Basij plays an active and increasing role in Iran's cyber-related struggles against the West. The commander of the IRGC unit in Qom, Iran, said in September 2010 that 2,000 Basijis had been trained in blogging and cyberwarfare.[71] A year later, the commander of an IRGC unit in Tehran claimed that 15,000 Basij members had been taught how to blog, although his superior said that only 2,000 of them had been trained in "cyberwarfare."[72] In September 2013, the cultural operations deputy of the Cyberspace Base of the greater Tehran IRGC unit inspected the cyber capabilities of the Basij Qods Resistance Zone.[73] The formal military language of this announcement indicates the degree to which the IRGC sees Basij cyber activities as core parts of its security mission and, effectively, elements of military power.

The Basij also maintains much of the IRGC cyberinfrastructure that is publicly accessible. Each of Iran's 31 provinces has its own provincial IRGC unit, to which the provincial Basij force is subordinated. These provincial units maintain websites, generally in the form "province_name.basij.ir" The websites themselves, however, belong to the provincial IRGC units and not just the provincial Basijis.[74] They are therefore somewhat analogous to the websites that American military units and bases maintain to serve local communities and service members and provide news about the units' activities.[75] These are the actual IRGC provincial websites and constitute the bulk of the open IRGC military online infrastructure.

All but two of these sites are hosted on IPs in the range 212.80.20.0/23, with 22 provincial sites residing on 212.80.20.238 and the remaining seven on their own IPs in this range.[76] The exceptions are the sites for West Azerbaijan and Fars Provinces, which are hosted on completely different commercial infrastructure.[77] Some provincial units use URLs that differ from the standard naming convention. The Kerman Province unit, for example, is saeir(.)ir, the Fars Provincial unit is tanvir(.)ir, and Tehran's is sepahostantehran(.)com. In each case, however, there is a server located at the normal address [Kerman(.)basij(.)ir, fars(.)basij(.)ir, and Tehran(.)basij(.)ir] running the same software: Apache 2.2.23 (CentOS) and PHP/5.2.17, both relatively recent versions of web server software. It appears that servers were set up for every province by some central organization, but some provinces preferred to use their own domain names and/or Internet infrastructure.

The central organization that set up all the servers was most likely a company called Ertebat Gostaran Bina, which owns the autonomous system 50733. This autonomous system is interesting because it controls only the IP range used by these IRGC provincial sites—212.80.20.0/23.[78] Ertebat Gostaran Bina is close to a ghost organization when it comes to web hosting, although its website, binaertebat(.)ir, boasts a number of computer hardware-related services (especially closed-circuit surveillance cameras) as well as web hosting and a number of software development services.

It does not appear to host any other IP addresses or websites, and it has so far been impossible to identify its leadership, let alone its ownership. It registered on the Regional Internet Registry organization that covers the Middle East and Europe (Réseaux IP Européens, or RIPE) with a physical address in a neighborhood close to the main IRGC and Basij bases in western Tehran—which is different from the directions it gives to its location on its own website. Given this location and the fact that it only seems to host IRGC and Basij systems on a very small network, it seems likely that Ertebat Gostaran Bina is either a front for or controlled by the IRGC or Basij and that it provides web-hosting services on dedicated systems only for them.

The difference between Ertebat Gostaran Bina and the companies hosting the websites of West Azerbaijan and Fars is instructive in this regard. The West Azerbaijan provincial website is hosted by Afranet, one of the larger Iranian ISPs, while that of Fars is managed by Aria Shatel and Iran Samaneh, also established ISPs. The West Azerbaijan site is on an IP address with 25 other websites belonging to different organizations, part of an IP range with hundreds of different domain names belonging to all sorts of entities. It looks, in other words, like a relatively normal commercial provider. The Fars site is a little more odd, as the IP range it is on is dominated by major news outlets, including that of *Kayhan,* which is closely affiliated with the supreme leader, and their mail servers. Its own IP address, 94.182.146.85, also hosts a number of other Fars Province Basij-related websites and their mail servers. This IP range (94.182.146.0/24) appears to have been largely reserved by a commercial ISP for the use of mostly state or state-supported organizations. The Ertebat Gostaran Bina arrangement, by contrast, looks more similar to the way a government entity, university, or large company builds its corporate systems. It does not look in any way like a normal Internet service provider, even one facilitating the hosting of websites belonging to or favored by the regime.

We must evaluate the more than 1,360 attacks against Norse sensors from the IP ranges hosting the IRGC provincial and Basij national infrastructure within this context, therefore. Standard arguments against attributing attacks from commercially hosted IP addresses to specific entities using those IP addresses lose much of their force in the face of the evidence that this entire cyber ecosystem is controlled by the IRGC. It seems very likely that these attacks are deliberate IRGC undertakings.

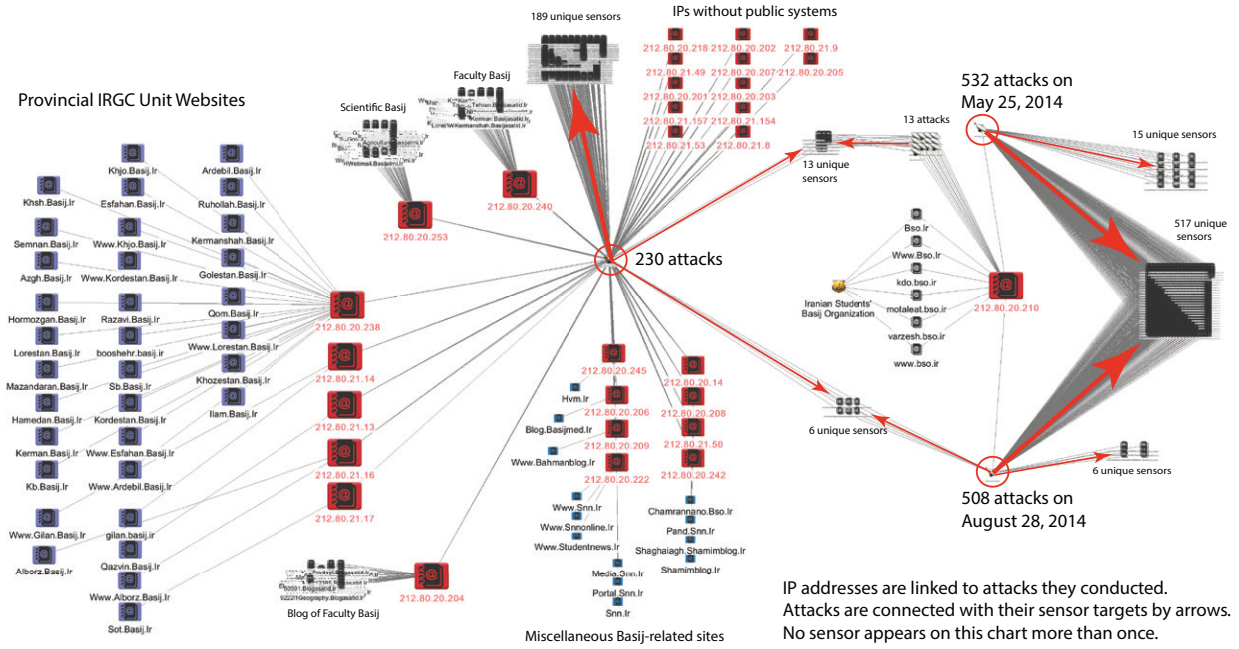
The attacks themselves break down into three major groups of events. Automated attacks originating on 212.80.20.210 on May 25 and August 28, 2014, generated 532 and 506 incidents, respectively. A total of 29 IP addresses conducted another 230 attacks between January 1, 2014, and March 17, 2015. The dispersion of these attacks over a long period of time, generally not more than three or four on any given day, suggests that they were conducted manually rather than by a hacking script.

The automated attacks from 212.80.20.210 were attempts to reconnoiter systems that could be compromised and used to attack still other systems. They hit only port 3389, used for remote desktop protocols and subject to vulnerabilities that could allow an attacker to take full control of the victim. They originated from 1,061 unique source ports, each used only once. The source ports broke into two general ranges. During the May attack, they included port 3064, every port between 4682 and 4959, and every port between 5531 and 5655, then almost every port between 5670 and 5809, followed by smaller ranges (generally five at a time) of consecutive higher ports. The August attack showed a similar pattern only with higher ports—generally between 38379 and 30092. The attack in May hit 532 unique Norse sensors with no repetition; the August attack hit 529 unique sensors without repeats. Both attacks, however, hit 517 of the same sensors, while 37 sensors were hit only a single time.

Each attack lasted a total of less than 20 seconds. Both times, however, 508 of the attacks occurred within four seconds, for an average of 127 attacks per second during those bursts. That rate of fire guarantees that the attacker was automated. It also suggests that each attack was launched without waiting for a response to the previous attack. It would normally take between 30 and 60 milliseconds for a message to travel from one system to another and back again, which would make it possible, theoretically, for between 16 and 32 round trips per second. Iran is nearly 10,000 kilometers from

FIGURE 11

CYBERATTACKS AND IT STRUCTURE OF IRGC PROVINCIAL UNITS AND BASIJ SYSTEMS



Sources: Norse database, provincial and Basij websites

the US, however, and Internet data move at or below the speed of light, which is 300 kilometers per millisecond. A data packet, therefore, must take at least 33 milliseconds to move from Iran to the US—66 milliseconds for the round trip. An attack launched at the rate of 127 per second could not even reach its target, let alone receive a response, before the next attack was dispatched.

The point of this excursion into optical physics is that these attacks were not meant to find one vulnerable system and stop, or even to determine whether one target was vulnerable before moving on to the next. It is highly unlikely that they were meant to compromise the target system, in fact. They were, rather, an effort at widespread reconnaissance to find as many systems that might be vulnerable to a particular exploit as possible in a very short period of time. They were also subtly designed and executed—each target system was hit only twice, with the events separated by three months. From the standpoint of the targets, such traffic is hardly worth reporting and would not stand out in security logs. That is probably why there are virtually no other reports of malign activity attributed to this IP address—it may have hit many other systems, but its attacks would have been buried in the noise of less subtle efforts and normal traffic. They only stand out as noteworthy to us because they hit many Norse sensors and thereby created a pattern invisible to almost any other network security systems.

It is likely that the Basij Student Organization was responsible for these attacks because it is the only organization hosting servers on 212.80.20.210. If this assessment is correct, it corroborates the claims of IRGC commanders that they are mobilizing Basijis and students in support of their cyberwar efforts.

The other 230 attacks from this IP range took a very different form, although with some common features (figure 11). They were conducted a few at a time rather than in intense bursts and over a long period rather than at a concentrated moment. They originated

from 29 different IP addresses rather than one. They all passed through source port 53 and hit 199 different destination ports, 27 of them two or three times. More than 200 unique Norse sensors were involved, of which only six overlapped with the sensors hit by the May and August automated attacks. (Another 13 were hit at other times by the originator of those automated attacks.) Norse sensors emulate different kinds of IT systems and employ a high degree of artificial intelligence to diversify how they are represented to adversaries in response to their actions, so it is not surprising that there should be very little overlap between attacks aimed at exploiting remote desktop control protocols and those engaged in other kinds of reconnaissance, as these 230 attacks seemed to be.

Attributing these attacks to specific components of the IRGC or Basij is more complicated. All of them originated on IP addresses owned by Ertebat Gostaran Bina and hosting only Basij or IRGC infrastructure. Twelve came from IP addresses with no visible infrastructure; the other 17 were scattered among systems belonging to provincial IRGC units and provincial elements of Basij organizations embedded in universities, schools, and other civic groups, as well as some components of the national Basij organization. The data do not permit further analysis to discern whether some provinces were more active than others, for example, since the different components of the Basij organization tend to host many provincial websites on the same IP addresses. It is possible that these attacks were conducted by multiple individuals using each site separately. It is also possible that someone compromised a number of these systems, which feature relatively outdated versions of web server software more likely to be vulnerable to exploitation, and used them to mask his own attacks on Norse sensors. A last possibility is that the attacks were injected at the autonomous system level and made to appear as though they originated with these particular IP addresses.

The only scenario in which the attribution of these attacks to the IRGC or Basij could be seriously questioned is the second—that a number of systems with older software were compromised. Even this scenario would provide limited exculpation, however. Only some of the systems involved showed any indication of vulnerabilities. Some were buttoned tightly, denying all attempts to crawl them. Others, including the server from which the mass automated attacks originated, had up-to-date versions of server software installed. The fact that server software is outdated, moreover, is not evidence that it has been compromised—only that it could have been. It is at least as likely that some individuals with proper access to these systems were deliberately using them to reconnoiter Norse sensors.

It is possible that someone was freelancing—that the attacker was a "rogue actor" operating without the knowledge or consent of superiors in the IRGC or the regime. Such explanations are often deployed in attempts to exculpate the Iranian regime from aggressive activities, even when the rogue actors are uniformed members of the Iranian military. It is even easier to make such a case in the cyber realm, of course, and to dismiss these sophisticated and dangerous attacks in that way.

There is absolutely no evidence to suggest, however, that an unauthorized person or persons gained access to the IRGC's cyberinfrastructure and used it to attack Norse sensors against the desires of the owners of that infrastructure. The public commentary by IRGC officers about their active undertakings to train and deploy Basijis in their cyberwar efforts are evidence in the other direction. The IRGC says it is using Basij members to attack the West, Norse observes sophisticated attacks from Basij and IRGC IP addresses, and no evidence suggests that most of those systems were compromised from outsiders. The soundest explanation is that these attacks are part of a deliberate IRGC campaign to identify vulnerable computer systems in the US for later compromise and exploitation.

Attacks from Sharif University of Technology. Sharif University is one of the premier technology schools in Iran. Founded in 1966, it now claims 300 full-time and 430 part-time faculty and 12,000 students.[79] Its graduates are sought after not only in Iran but also in the US and Canada as well.[80] Its 13 academic departments focus heavily on engineering, including aerospace, chemical and petroleum, materials science, and computer and electrical engineering. Its computer engineering department dates back

to 1970, with a PhD program starting in 1997.[81] It also boasts a number of research centers, including the Center for Excellence in Design, Robotics, and Automation; the Entrepreneurship Center; the Center of Excellence in Aerospace Systems; and the Advanced Information and Communication Technology Center (AICTC). It is part of Iran's venture into nanotechnology, hosting the Research Center for Nanostructured and Advanced Materials since 2004.[82] Its involvement in nanotechnology is of particular interest because miniaturization is one of the most important and difficult aspects of turning a nuclear weapon into a usable missile warhead.[83]

Sharif University is also the subject of international sanctions. The US Treasury Department sanctioned three organizations at the university for proliferations-related activities in 2012: the AICTC, the Digital Media Lab, and the Value-Added Services Laboratory.[84] The European Union sanctioned all of Sharif University in 2012, a decision annulled by the General Court of the European Union in July 2014. The EU reinstated many sanctions, however, in November 2014. The Canadian government designated Sharif's Department of Engineering in December 2012.[85]

The US Treasury Department aimed directly at Sharif's computer programs in 2012 for human rights abuses. It sanctioned Rasoul Jalili, then-dean of scientific and international cooperation and head of the Information Technology Group at Sharif and one of the founding members of the Iranian Supreme Council of Cyberspace, appointed by Khamenei in 2012.[86] Jalili was sanctioned for "attempting to acquire equipment related to monitoring of SMS traffic from abroad" and "actively assisting the Government of Iran's censorship activities."[87] He also "assisted in blocking any website that contained content criticizing the Iranian Government," and his company, AmnAfzar Gostar-e Sharif, also sanctioned, "provided Internet censorship and filtering software to the Government of Iran." AmnAfzar produced monitoring and filtering equipment and software including the Separ, Saran, Squid Escort, and Alal Web Filters, according to the US Treasury Department. Separ is reportedly "capable of real-time inspection of transmitted data, deep URL inspection . . . and includes real-time monitoring capabilities." Jalili remains on the faculty at Sharif but was removed from his position as dean in April 2012.[88]

This background gives context to a sophisticated and heavily obscured cyberreconnaissance operation executed by Sharif University systems between September 2013 and the end of August 2014. Norse sensors have identified 1,580 attacks from systems openly registered to Sharif from September 1, 2013, to March 17, 2014, about half of which were involved in this reconnaissance.

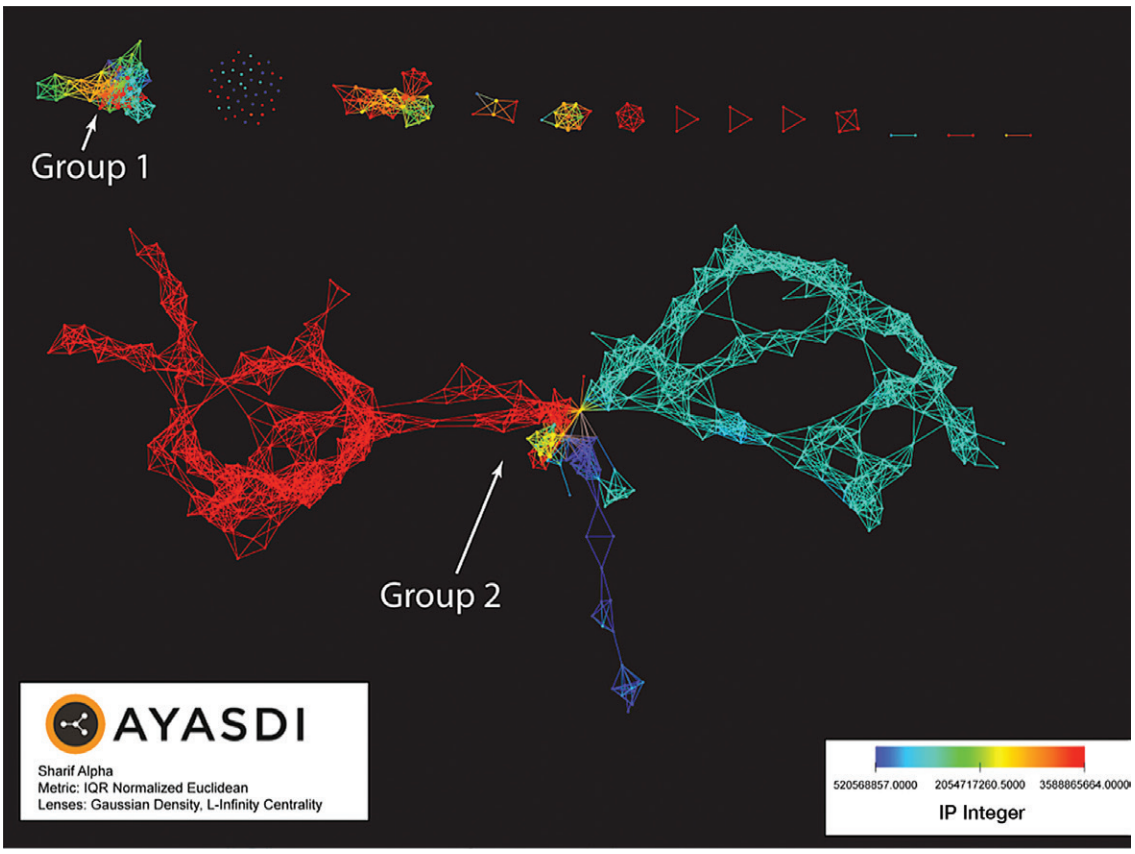
To identify the patterns within these attacks, we used a unique visualization tool called Ayasdi Core. Ayasdi Core can examine a collection of cyber events defined by the source and destination IPs and ports, dates, times, and protocols (and other information if desired) and form them into clusters or nodes based on their similarity to one another. Individual events are likely to appear in more than one cluster or node because they are likely to be similar to certain events in some ways and to other events in others. An event could be placed in a node with other events that happened at around the same time, but it could also appear in a different node with events using the same IP address or ports that occurred at different times. In these cases, Ayasdi Core draws a line between the two nodes. It then creates a visual representation of these nodes and the links between them, from which one can discern patterns that might be interesting to explore further.[89]

Comprehending an Ayasdi visualization requires some explanation and practice. The location of nodes on the graph and the length of links between them are irrelevant. The size of the nodes indicates how many individual events are in each. The color of a node depends on how many events in that node contain a particular value of a particular data element such as IP address or date. Figure 12 is colored according to IP address, with each node taking on the color assigned to the IP address to which most of the events in that node belong.

The graph reveals one large and complex group of nodes (group 2) dominated by IP addresses tightly concentrated in three ranges (red, teal, and blue), with a few nodes in other ranges or with intermingled IP addresses. It also shows a second dense group of nodes (group 1) with many colors spread all through it, indicating that a

FIGURE 12

VISUALIZATION OF SHARIF UNIVERSITY ATTACKS ON NORSE SYSTEMS



Source: Norse database visualized using Ayasdi Core

number of events with very different IP addresses are all linked by some other factor. The smaller groups repeat this phenomenon with many fewer events.

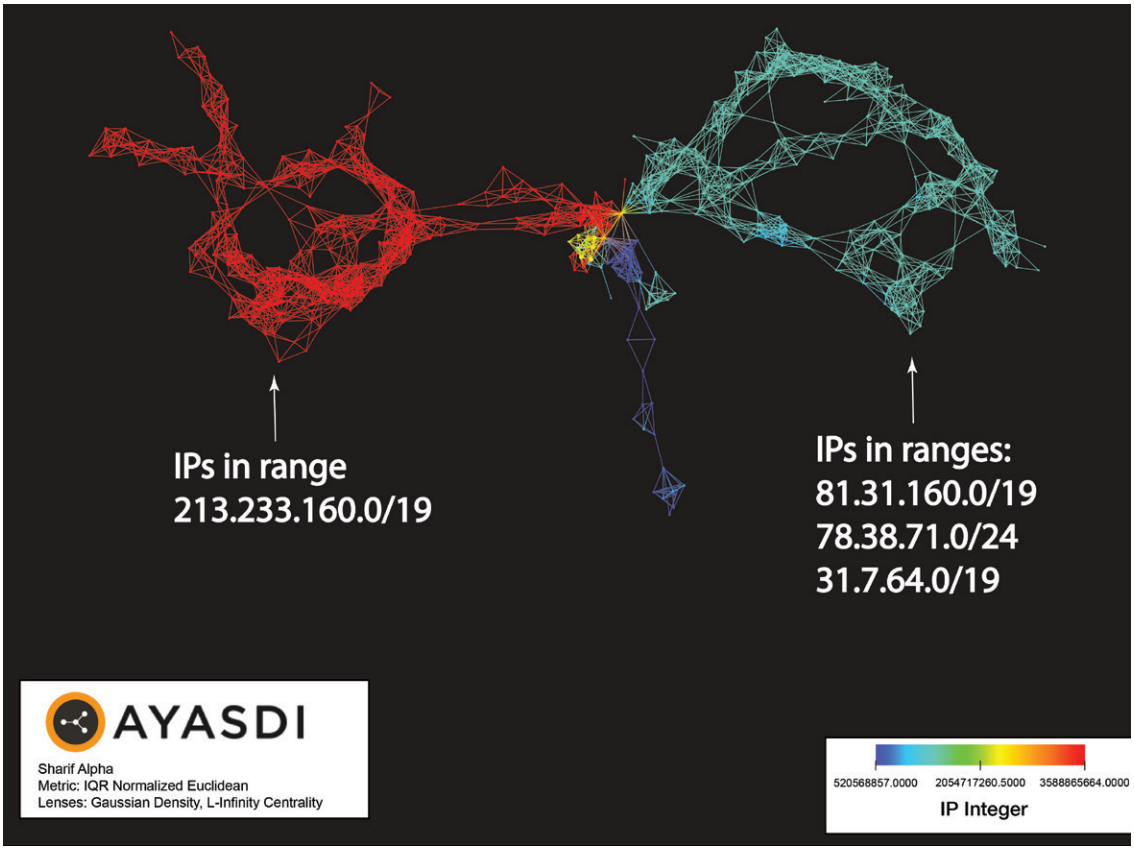
Examination of the underlying data shows that all of the events in group 1 used the same source port: 53. The 249 events in this group are, in fact, part of a port scan conducted by systems on several IP addresses trying to find vulnerabilities by trying many destination ports to see if any are open. Such firewalking can be interesting, but the larger and more complex pattern of group 2 deserves our attention.

Group 2 includes 1,118 attacks from more than 126 IPs registered to Sharif University. The nodes are colored by IP address, showing clearly that there were two major groups of IPs (red and teal) and one smaller group (blue) of IPs involved in the attack (figure 13).

Ayasdi visualizations often have three kinds of distinctive features: lines, flares, and loops. Lines of nodes generally suggest a progression of the data along some axis—successive events in time, for example. Flares indicate sets of data that start with some commonality and then diverge—a series of events might start at roughly the same time from similar IP addresses using the same ports, but the ports on one set of IP addresses might increase over time while those of another set decrease. Loops indicate cyclical data. The same general collection of ports used repeatedly over the course of many days or months, for example, could produce a loop. The shapes of the red and teal groups indicate cyclic but irregular patterns in the data. Some element

FIGURE 13

IP RANGES FROM SHARIF UNIVERSITY ATTACKS



Source: Norse database visualized using Ayasdi Core

of the events kept changing but with repetitions of some sort over time.

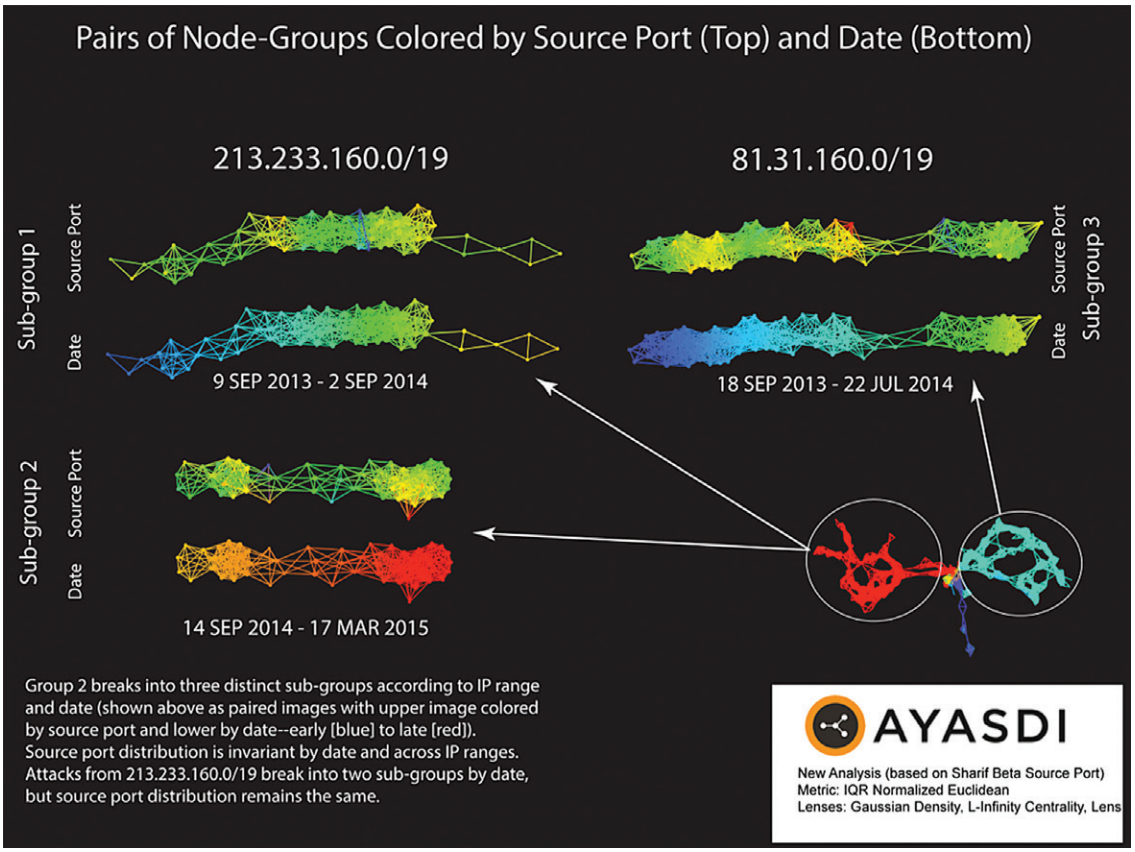
The common element binding these nodes appears to be that they all were directed against port 445, regardless of their source, target, or date. Port 445 has long been a target of malware and remains a potential vulnerability for poorly secured machines. Gibson Research Corporation reported in 2008:

> Malicious hackers have been having a field day scanning for port 445, then easily and remotely commandeering Windows machines. Even several hackers I have spoken with are unnerved by the glaring insecurities created by port 445. One chilling consequence of port 445 has been the relatively silent appearance of NetBIOS worms. These worms slowly but methodically scan the Internet for instances of port 445, use tools like PsExec to transfer themselves into the new victim computer, then redouble their scanning efforts. Through this mechanism, massive, remotely controlled Denial of Service 'Bot Armies', containing tens of thousands of NetBIOS worm compromised machines, have been assembled and now inhabit the Internet.[90]

This port was among those used by the Conficker virus that spread so rapidly and broadly across the Internet in 2009.[91] Hackers continue to discover new ways to exploit this port, as a recent Microsoft security patch highlighted.[92] Iranian attackers going after port 445 are likely preparing for something very nasty indeed.

FIGURE 14

IP RANGES FROM SHARIF UNIVERSITY ATTACKS, COLORED BY SOURCE PORT AND DATE



Source: Norse database visualized using Ayasdi Core

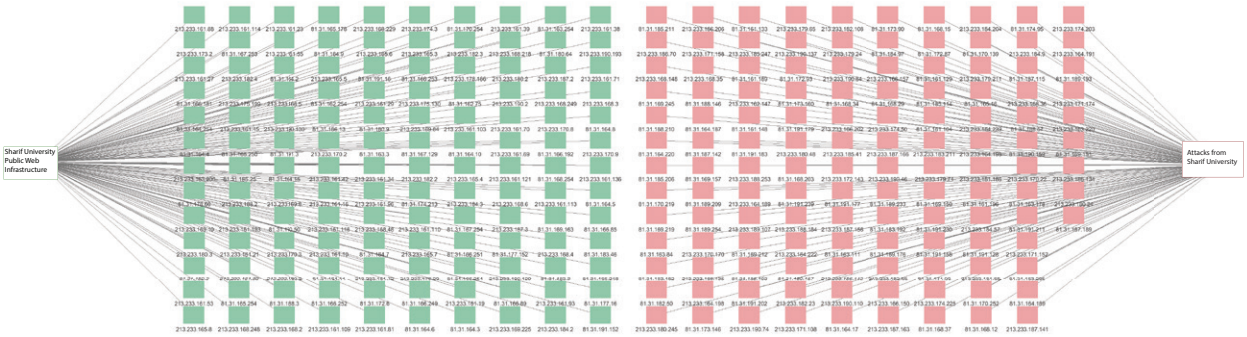
Ayasdi also has the ability to reshape the visualization by focusing on a particular element of the data, which it calls a "data lens." We applied a data lens focused on the source port of the events to produce a chart and colored it according to source port (figure 14). Group 2 from the original chart is here, broken into three subgroups of very similar color patterns (yellow-green), showing that all of these IPs used a common selection of source ports ranging from 1037 to 4987 (with a handful of outliers).

The clusters themselves are distinguished from one another by the IP address ranges of the attacker. The visualizations clearly show multiple IP addresses from two different address ranges all using virtually the same set of source ports to attack the identical destination port. Closer examination of the data shows an additional pattern—in almost every case, the attacking IP hit its target from the same port twice within two to three seconds. In most cases, each IP conducted only one such paired attack. The attacks hit sensors on 56 different IPs in Australia, Bulgaria, Germany, France, Britain, Liechtenstein, Portugal, Russia, Thailand, Turkey, and the US.

The value of compromises using port 445 increases with the number of computers that can be effectively spoofed. It makes sense, then, that the attacks emanating from Sharif University hit so many different sensors. These attacks do not necessarily harm the target machine but, rather, represent an early-stage effort to develop a compromised cyberinfrastructure from which

FIGURE 15

SHARIF IP ADDRESSES WITH PUBLIC-FACING SYSTEMS (GREEN) AND MALWARE ATTACKS (RED)



Source: Norse database

to conduct future attacks of another variety. There is no way to know if the operation stopped because its controllers gave up on it, were caught somehow that has not made its way into the news, or simply obtained enough compromised systems to satisfy themselves. Considering the duration and breadth of the attacks, it is improbable to the point of nullity that they were unable to compromise any systems.

Attributing these attacks to Sharif University is superficially straightforward, since the attacks all originated from infrastructure openly registered to Sharif. The fact that they originated from so many different IP addresses in so many different networks, however, argues against the likelihood that individual humans were actively sitting at each specific system to conduct these attacks. The precision with which the attacks hit from the same port twice in very close succession suggests automation, moreover. The next level of superficiality, therefore, suggests considering the possibility that Sharif's systems were infected by a botnet and that Sharif was the victim rather than the perpetrator.

We explored this hypothesis by first examining the results of Norse crawls of the IPs in question, which turned up a handful of systems with outdated software that could have been compromised (as well as a few that had been recently updated and were unlikely to have been compromised). We discarded the few that might have been victims and concentrated on those that remained.

These presented another interesting pattern. In figure 15, we mapped all visible domain names belonging to Sharif University to their IPs (IPs in green) and compared the resulting relationships with the IPs from which the malware originated (IPs in red).

It emerged that not a single case of malware originated from an IP that hosted overt Sharif systems. Almost all of the attacking IPs, on the contrary, show no visible infrastructure. This correlation is the inverse of what we would expect if Sharif's systems had been compromised by a botnet spreading randomly across campus. The distribution of such an attack should be either random or concentrated on visible infrastructure, which makes the easiest target for automated hacking. One might imagine a botnet programmed to infect only empty IPs and thus avoid compromising or damaging Sharif's systems, but that would suggest that it was designed by someone affiliated with Sharif who was concerned about the welfare of those systems.

The structure of Sharif's IT systems, however, offers a simpler explanation. Sharif maintains its own autonomous system, AS12660, which routes traffic through AS12880 and, in the past, also AS6736. Autonomous system 12880, we should recall, is the principal gateway between Iran and the global Internet and the

regime's main monitoring and filtering system. AS6736 is used by only a small number of universities and government research organizations and is very likely also monitored very closely. It would be relatively easy for someone with direct access to AS12660 to inject traffic at the autonomous system that appeared to trace back to IPs it announced. It is possible that an outside hacker penetrated the autonomous system itself and injected this traffic. But why would such a hacker have been so fastidious about not falsely attributing his traffic to addresses with Sharif University public systems on them? The most likely explanation, therefore, is that the spoofing was done deliberately by someone working for and in the interests of Sharif with administrative access to the autonomous system.

Acquiring such infrastructure would facilitate malicious activities on a larger scale, in ways that could be extremely difficult to attribute to Iran.

Could that someone have been a rogue actor, using Sharif's systems for his or her own purposes? That is possible but not likely. The Iranian government, as we have seen, pays special attention to Sharif's systems and apparently has enough confidence in the degree to which they are monitored and controlled to lift throttling restrictions at sensitive times more rapidly for Sharif than for other institutions. Yet Sharif's traffic still passes through the regime's monitoring systems, as we have noted. Had these attacks occurred in a short period of time, it might be possible to imagine someone going rogue for a bit. It is extremely unlikely, however, that a rogue actor would have been able to maintain this kind of operation on such sensitive and carefully monitored systems for nearly a year.

The attacks were stealthy, to be sure. Few, if any, cybersecurity analysts would pay attention to a double tap, even on port 445, from a single IP that is not repeated or where any repetition comes from a different IP months later. They were also stealthy from the standpoint of the original individual systems—most IPs conducted only one double attack in the entire period. They were not, however, as stealthy from the standpoint of the autonomous systems through which they ran and where all of this traffic would have been aggregated. The logs of those systems must show several thousand pairs of interactions between Sharif's systems and targets. It is possible that the network security teams working for Sharif and at AS12880 and AS6736 missed this traffic and also missed any other indications that someone was misusing a sensitive system—but it is just not very likely.

We assess with moderate confidence, therefore, that one or more officials in positions to control Sharif's network deliberately ordered (or tolerated) a widespread, systematic, and stealthy effort to probe Western infrastructure for future attacks. Acquiring such infrastructure would facilitate malicious activities on a larger scale, in ways that could be extremely difficult to attribute to Iran. Considering the well-known connection of a very senior Sharif computer professor and center director with the Iranian government, and the university's overall very close relationship with the Iranian security services, it is very likely that this effort was undertaken on behalf of the Iranian regime.

Systems without Owners, but Supporting the Regime

Attacks on Norse sensors originating from Iran fall into three categories, as we have noted: systems belonging to individuals, systems belonging to institutions, and systems seemingly belonging to no one. Now we will focus on that third category.

A large number of attacks picked up by the Norse Intelligence Network originate from servers that do not appear to belong to anyone—that is, blocks of IP addresses registered to ISPs but lacking any websites, email servers, nameservers, or other systems typical of commercial application. Careful examination of some of these events and systems, however, suggests that the attackers using these servers identify with the regime's ideology.

At least one of the incidents coincided with #OpSaveGaza, a cyberattack against Israel organized by

social media that generated a large increase in attacks from Iran. We assess with moderate confidence, moreover, that individuals with administrative access to the corporate systems of two Iranian ISPs conducted these attacks against Norse systems—or the Iranian regime itself conducted the attacks and made them appear to have originated from these ISP systems. We assess with low confidence, therefore, that these attacks from seemingly unattributable systems were conducted by regime agents or supporters.

Attack on a Norse Sensor. On July 12, 2014, systems on seven IPs located in Iran attacked a single Norse sensor more than 1,000 times in 11 hours (table 2).

These attacks were attempts at "firewalking," an automated procedure used to identify which ports and services on a firewall are accessible to outside traffic and then to penetrate that firewall through those ports or services.[93] Their targets were seemingly randomly selected high ports between 49157 and 65530 (all of which are dynamically assigned—that is, they do not have permanent or semipermanent assignments to particular services). The source ports were much more narrowly chosen, with 223 attacks originating from port 53, one of the standard ports often used for firewalking because many firewalls are configured to allow traffic from that port through without checking it. The rest of the attacks originated on ports between 10003 (with 300 incidents) and 23886 (with 29).

All of the attacks from port 53 originated from two IPs, 89.165.0.14 and 178.234.40.253, and those two IPs used only that port to attack from. These attacks hit a total of 220 distinct destination ports with only two overlaps. It is therefore possible that there were two distinct attacks against this Norse sensor at the same time, one from these two IPs and the other from the remaining five. The timings of the attacks suggests that they were not conducted by a botnet. The pattern is irregular, with generally fewer than 10 attacks per minute (whereas a botnet usually spurts five or more attacks in a matter of seconds). It appears that one or more individuals were actively using these systems to reconnoiter this Norse sensor aggressively.

The two IPs that used port 53 exclusively had pinged this Norse sensor as early as April 22, 2014, but touched it only 26 times between then and the massed attack on July 12. They then abandoned it, suggesting that someone had decided to try to break into the sensor for a day and then moved on to greener pastures when he failed. There could well have been more than one individual involved because the two source IPs are more than 450 miles apart—one is in Tehran and the other in Mashhad, near the eastern border of the country.[94] If two people were involved, however, they must have coordinated closely.

TABLE 2

ATTACKS AGAINST NORSE SENSORS ON JULY 12, 2014, BY IP ADDRESS

IP Address	Attacks
95.82.111.179	274
95.82.104.126	181
95.82.99.191	176
178.236.40.253	176
95.82.104.98	140
95.82.111.153	92
89.165.0.14	47

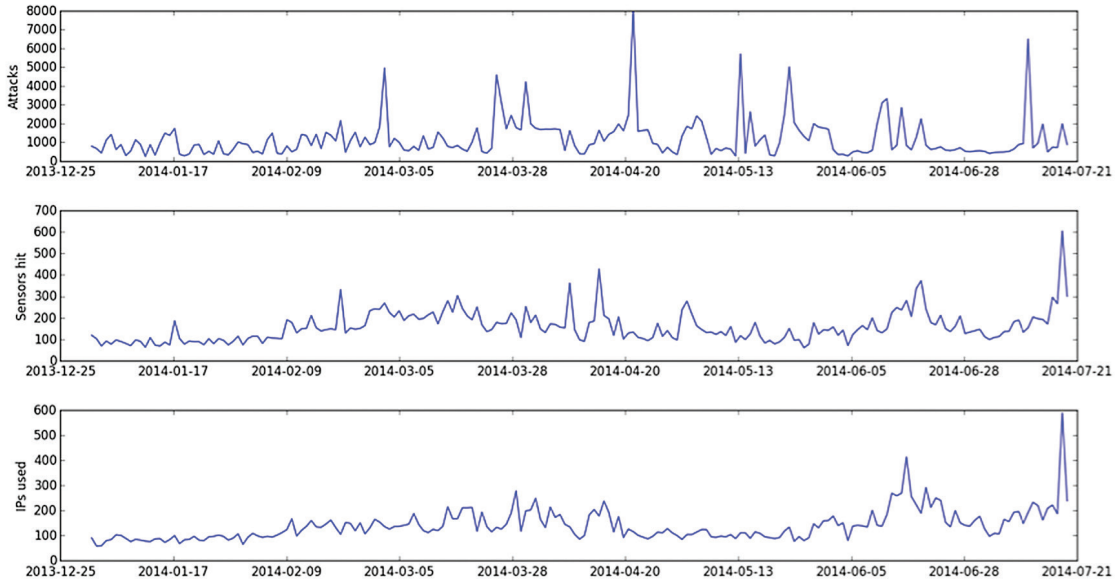
Source: Norse database

These two IP addresses, interestingly, host parts of the corporate infrastructure of the ISPs that own them and are not part of the address blocks those companies use to host clients.[95] Norse crawls of both IPs failed, indicating either that no systems are there or that they are blocking the crawls very effectively.[96] We can conclude with moderate confidence that one of two things is going on. Either individuals with administrative access to the corporate systems of two Iranian ISPs conducted an attack on a Norse sensor, or the regime itself conducted the attack and made it appear to have originated from these systems, both of which route their traffic through AS12880.

The other alternative—that both IPs were hacked, hijacked, and used to conduct the attacks by some third party—is far less plausible. A compromised system would very likely have responded to Norse crawls, not only because of the compromise but also because it would have had to have been both available and

FIGURE 16

ATTACKS FROM IRANIAN SYSTEMS AGAINST NORSE SENSORS, JANUARY–JULY 2014



Sources: Norse database.

vulnerable to be compromised in the first place. These systems appear to be very well-defended, with common ports buttoned up and the ability to block crawls. The likelihood that they were compromised by a hacker from outside of Iran is extremely remote, since that hacker would have had to penetrate the 12880 firewall to get to these well-protected systems in the first place. An individual inside Iran might have had a better chance to compromise them, since his traffic would not necessarily flow through 12880. He would still have been attacking IPs hosting the corporate infrastructure of two ISPs, however, and subject to the scrutiny of the general Iranian Internet monitoring system. There are many easier and less risky target systems in Iran to compromise for the purpose of attacking an American node, however.

It is easier to explain the timing—and, therefore, the motivation—of the attack. Israel launched Operation Protective Edge on July 8, 2014, conducting air attacks on more than 200 sites in the Gaza Strip in response to a prolonged campaign of Hamas missile attacks against Israel.[97] Hackers wasted no time in responding, announcing #OpSaveGaza and #Intifada_3 on Twitter and promising massive attacks against Israeli systems peaking on July 11.[98] The campaign used Twitter and Facebook to provide lists of target sites and succeeded in defacing more than 2,500 websites, shutting down many others, and leaking some data.[99]

Attacks from Iranian systems on Norse sensors spiked on July 12 after having been relatively low for three weeks (figure 16). The number of different IPs being used to attack Norse sensors did not increase significantly until July 18, however, which is also when the number of different sensors being hit increased markedly. The attacks we have been considering came right at the beginning of this cyber campaign. That fact suggests that the attackers already had access to these systems and were extremely responsive to the social media calls to avenge Gaza.

SCADA Attacks. Attributing the attacks from the other five aggressive IPs is much more difficult, but

more important because they appear to have been attempting to compromise SCADA systems.[100] They span three networks, none of which have ever been formally assigned to any individual or organization. But their routing paths have changed over time in a common pattern that is noteworthy. They had been routed through various autonomous systems prior to March 2014 but then were visible to the global Internet via AS48359 from March 15 to June 18 and again from July 25 into early 2015, when they switched to other systems. The data do not confirm that these systems were routing through AS48359 on July 12 during the attack, but they do not offer any indication that they were not. We shall proceed on the hypothesis that they were all using that system, therefore, with the caveat that we do not have proof.

This autonomous system belongs to a small ISP in Kermanshah, near the border with Iraq, called Internet Hesabgar ["calculator" or "calculating" in Farsi], run by Masoud Korani. Not much information is available on Internet Hesabgar apart from its own announcements of its provision of WiMax services to Kermanshah and, purportedly, other locations in Iran. It is possible to trace connections from some of its self-identified employees and former employees to potentially suspicious contacts, but the evidence is simply too tenuous to draw any meaningful conclusions.[101]

These IP addresses conducted three attacks that could have been targeting SCADA systems using three different ports against three different sensors. The ports (50020 and 50021) are used by Siemens Spectrum Power Transmission Grid control systems.[102] All three attacks came amid large-scale firewalking efforts coinciding with raised tensions with the West in April, July, and September 2014. Tehran attempted to appoint a former hostage taker as its permanent representative to the UN in early 2014, starting a diplomatic row leading to passage of legislation in Congress banning him from entering the country, which President Obama signed April 18. The second incident corresponded with the #OpSaveGaza campaign on July 12. The third incident followed shortly after Iran shot down an Israeli drone over Natanz (which it reported on August 24) and the release of the IAEA's September 5 report saying that Iran was not in compliance with its obligations to the agency to explain the possible military dimensions of its nuclear program.[103]

It is possible that the July attacks were simply part of the firewalking exercise, which, by its nature, hits many ports in this range rapidly. It is also possible that they were deliberately inserted into the scan in an effort to blend into the traffic. In the course of several hundred thousand attacks, after all, ports used by SCADA systems were hit fewer than 70 times, suggesting that they are not normal elements of a scan. There is no way to know for sure, but if the sensor had, in fact, been vulnerable SCADA software, these probes could have led to a serious compromise.

Another IP address did conduct what looks like a determined attempt specifically aimed at compromising SCADA software on September 5, 2014. Someone used IP 2.179.239.90 to conduct 62 attacks in 10 minutes against port 5051, which is used for the Telvent OASyS DNA system, the foundation on which all of Telvent's SCADA infrastructure is built.[104] Telvent was the victim of a significant attack attributed to Chinese hackers in September 2012.[105] This attack breached Telvent's "internal firewall and security systems . . . and stole project files related to" OASyS SCADA. It is concerning because Telvent systems are used heavily in operating and monitoring electrical grids.

It is possible that the Chinese were at it again two years later using compromised Iranian systems, but it is unlikely. The Iranian IP hosts no visible infrastructure and is apparently owned directly by the Telecommunications Company of Iran, running on AS12880. There has never been any public system identified with this IP, or with any of the IPs on this subnetwork, so there has not been any visible server to try to hack. Nor have the Chinese changed their methods from operating openly from their own infrastructure to using that of third parties. It is much more likely, therefore, that this was an actual Iranian attack designed to penetrate a SCADA system.

Critical infrastructure can be attacked in other ways, moreover, and Iranian hackers diligently follow the latest exploits that can give access allowing them to take control of remote systems. A vulnerability in a virtual network connection software used to allow remote access to a computer on port 5900 was revealed

in a major exposé in *Wired* in November 2013.[106] Researchers were able to use this exploit to access control systems for hydroelectric plants, as well as ventilation systems, security cameras, pharmacy records, and individuals' computers. Iranian systems attacked Norse sensors on port 5900 more than 2,400 times starting in September 2013.

The most aggressive systems originated on 95.142.225.90, owned by an ISP named Armaghan Rahe Talaie; 85.185.67.206, owned by Shahrood University of Technology; 78.38.114.220 (AS12880), owned by Zabol University of Medical Science; 213.233.170.91, owned by Sharif University of Technology; 188.121.120.19 (AS47796 via AS51074 via AS12880), ownership unclear; and 2.144.193.177 (AS44244), owned by Faragostar, an ISP.

The attacks we have described on port 5900 came almost entirely from corporate or institutional infrastructure.

The Sharif University address is interesting in light of our previous discussion of that university's likely role in a significant global reconnaissance occurring at the same time. There is no publicly visible infrastructure on 213.233.170.91 (AS12660 via AS12880), and Norse crawls during the attack period were stopped by some system on the other side (returned an error).[107] Other IPs in the same network host a great deal of infrastructure—all of it belonging to Sharif's computer engineering department. Systems hosted on this network include the main page for the department [ce(.)sharif(.)edu], two nameservers, and Sharif's webmail access portal.

The attacks from Sharif University's systems amounted to 46 incidents over the course of two weeks—too few and in too short a time period (second half of April 2014) to rule out either a compromise or a rogue actor. The attacks from Shahrood University, by contrast, numbered almost 1,300 spread over two months (March 21–May 19, 2014). This IP is also devoid of public infrastructure, but the encompassing network includes IPs hosting both Shahrood's main website and its mail server.

Attributing these attacks with any confidence is not feasible at this time. It is noteworthy, however, that many of them originated from subnetworks hosting corporate or institutional infrastructure. An ISP or hosting company, like any corporation, does not want to have its own corporate systems, including its payroll, email, banking arrangements, financial records, and so on, compromised. By separating its own systems from its customers', it can make the systems handling that corporate information as secure as it pleases. It generally cannot control as well the security of the websites or other public systems that its customers establish on its servers, however. Insecurities in those public-facing, customer-controlled systems can put the security of the server they are on at greater risk. Business prudence dictates keeping those systems separate from the corporate infrastructure the company needs to protect.

The attacks we have described on port 5900 came almost entirely from corporate or institutional infrastructure—the networks hosting the public websites and mail servers of Shahrood University, Sharif University Computer Engineering Department, and the Armaghan Company. That fact suggests that the attacker was not merely a student or customer compromising public systems. It was either someone with access to the institutional and corporate infrastructure of these organizations or an external attacker specifically targeting corporate rather than public systems.

IPs associated with those networks conducted a total of 2,243 attacks against Norse sensors between October 26, 2013, and May 18, 2014 (of which the attacks against port 5900 are a large subset). They follow a very consistent pattern. They are automated, regularly conducting more than 200 attacks per second. There is, therefore, some script or program executing these attacks. But the script does not just run itself. It stops at irregular intervals, restarting again a few minutes or a few hours later. Almost invariably, when it restarts it is attacking from a different source port than the one it had been using before. The conclusion is clear: a hacker was running the script and periodically stopping it; tweaking it to try attacking from a different port; taking breaks for breakfast, meetings, and—one hopes—the

periodic shower; and returning to the script. A human being, in other words, was almost certainly in full control of these attacks and consciously directing them to try to find a route to penetrate a vulnerable target.

The targets themselves are also interesting. These attacks hit a total of 894 different Norse sensors, generally a handful of times each over the course of several days or weeks. The attacks are grouped by country as well, so that a cluster of attacks hits a number of sensors in one country in an automated fashion, then breaks, then starts with a different set of sensors in a different country, which it also hits from a different source port and sometimes on a different destination port. Of those sensors, 801 were located in the US. The attack was therefore a determined effort to find vulnerabilities on US systems that would allow the Iranian hacker to take control of those systems, which would give him the ability to read or destroy their data and to use them for unattributable attacks on other systems.

These attacks are not likely the effort of a single hacker. The originating systems are in different parts of Tehran and also in Zahedan, an airplane ride away. For the most part, the intervals between when the attacks from one IP stop and those from another begin are long enough for someone to drive from one part of Tehran to another, or even to fly from Tehran to Zabol, although there is at least one exception that would require the attacker to be in two places at once. It is more plausible, therefore, that the attacks were conducted by a small team of hackers using the same or a similar attack script, operating from a common set of targets and a common standard procedure for alternating ports that evolved over time.

Returning to the infrastructure from which these attacks were launched, we must choose from three options: the traffic was injected at the level of autonomous system 12880, the only one all of these IPs have in common; a number of hackers with direct access to the corporate infrastructure of several IPs and universities conducted these attacks jointly; or most, if not all, of these systems were taken over by an external hacker despite a lack of indication that any of them were compromised. The latter option remains the least likely—the attacks occurred over a protracted period of time and generated enough traffic on each system to have been noticed by network security professionals who should have been monitoring the networks hosting their own infrastructure. They may have generated enough traffic collectively to have been noticed by careful monitors at AS12880, although they could simply have been buried in what must be an unmanageable volume of data moving through that system. We cannot say with any confidence which it was, but the involvement of Sharif's Computer Engineering Department systems suggests that we should look further into the possibility of regime support for this activity.

CONCLUSIONS

Iran has become a significant player in the cyberattack arena. Its threat is no longer confined to patriotic hackers defacing websites. Individuals, companies, and regime organs have all evolved sophisticated cyberattack capabilities and have developed global infrastructure with which to expand and improve them. These capabilities are more concerning because they do not appear to have been developed primarily for mercenary reasons. They seem, rather, to be used in the service of the security and ideological interests of the regime.

The Iranian attacks against Norse sensors, together with the attacks conducted against JPMorgan Chase, Saudi Aramco, and the Sands Casino, provide a glimpse into the motivations of the hackers. These attacks were clearly not profit-driven. They penetrated three wealthy organizations and sought to destroy data rather than steal intellectual property or money. The attack on Aramco served the interests of the Iranian state directly; the one on Sands seems to have been driven by Iranian nationalism. Significant increases in attack volume on Norse sensors generally correlate with rising tensions with the West and/or perceived attacks or insults to Iran.

Iran's cyberwarfare capabilities do not yet seem to rival those of Russia in skill, or China in scale. The community of high-end hackers in Iran remains relatively small and constrained to some extent by infrastructural limitations resulting from sanctions—and from the sheer difficulty of building a robust network in Iran's physical and political terrain. We have not seen evidence to suggest that Iran is capable of penetrating US national security or critical infrastructure systems outfitted with modern, best-practices cyberdefense systems.

The Iranian cyberthreat is not yet unmanageable, but it is growing rapidly. Iranian attack infrastructure (as measured by the number of IPs used to conduct attacks) has increased dramatically over the last two years, as has the number of attacks. Iranians have shown the ability to conduct sophisticated missions to find and compromise systems while leaving few footprints. They are deliberately training groups of hackers and directing them to support Iranian national interests. This training appears to incorporate a lot of unconstrained "live fire" exercises in which the trainees actually attack Western systems while learning their trade. Like any modern nation, Iran is heavily investing in its IT infrastructure and in IT education, with an eye toward building a large knowledge-based economy.

The relationship between Iran's universities, the state, and the hacking community is particularly worrisome because of the high quality and breadth of academic work seen from Iran's scholars. A full review of the Iranian cyber-related academic literature is beyond the scope of this paper but may be pursued as part of our ongoing research. The Iranian online community is also fully aware of advances and arguments within the global cyber community, as shown by citations in its articles and the alacrity with which Iranian hackers pick up on exploits reported by Western media. We project that Iran is likely to become a serious cyberthreat to nations that would oppose it, based on this strong intellectual and academic foundation.

It is also easy to see how the general doctrines and approaches of the Iranian security services and foreign policy organs are being mapped to Iran's new activities in cyberspace. Iran's hackers appear to move easily between ostentatious attacks and defacements and very quiet preparations for future operations, just as Iran's security and intelligence forces do. They maintain a similar two-track system of responding overtly to perceived attacks against Iran while continuing covert efforts to expand their abilities to conduct future attacks. They seem to prefer to operate as individuals or small groups with plausibly deniable links to the state, just as their militant proxies throughout the region do, as opposed to the overt state control China maintains over its hackers. Iranian hackers rarely claim to be fully independent of the state, like Russian "hacktivists" do, and acknowledge their relationship with state and security entities from time to time. In this respect they are like Shi'a militias in Iraq and Syria, who maintain their nominal independence from Iran while explicitly recognizing their relationships with Tehran, the assistance they receive from Iran, and their loyalty to Iran's values.[108]

The threat from Iran cannot be measured merely by the number of attacks they are conducting or even the

nature of those attacks. Historically, Iranian strategy values building up a base for future operations. Iranian security services prefer to penetrate as many organizations as possible—friendly, neutral, and hostile—in advance of when they might need to influence them. We should expect Iranian hackers to do the same.

What advantage does the Iranian state gain from this activity? Deterrence, presumably, and better tools with which to control the escalation of political or military crises.

The Iranian regime continues to seek effective deterrents to potential US or Israeli military strikes. Still, it is not confident—rhetoric aside—that it can build its own adequate conventional military defense any time soon. It has, therefore, developed a wide variety of other means by which to threaten to inflict pain on a potential attacker, ranging from the tens of thousands of rockets deployed in Lebanon and Gaza to the thousands of small boats and minelayers supposedly ready to close the Strait of Hormuz, to the missiles able to hit American military facilities throughout the Persian Gulf region. Cyberattack capabilities are obviously a significant addition to this deterrence and escalation-management arsenal, and one that might prove to be extremely cost-efficient in an asymmetric conflict against a major power.

In American strategic thinking, a US military attack on Iranian soil could be a proportionate response to an Iranian attack on an American military base in Bahrain or Qatar. The Iranians likely do not see things that way. For them, the proportionality would be meeting an attack on their homeland with an attack on ours—but such an attack will be beyond their conventional military capabilities for a long time to come. For Iran, a cyberattack is a promising avenue by which Tehran could bring any future conflict to American soil, especially since it offers a way to do so that is graduated and potentially unattributable and may or may not involve casualties and the destruction of physical infrastructure.

One thing is certain, however: any significant loosening of sanctions on Iran will facilitate Tehran's efforts to develop its cyberattack capability. Iran would almost certainly considerably augment its already-impressive ability to monitor and control its people while dramatically expanding its internal cyber capabilities. It is also likely to extend its international cyber footprint while continuing efforts to compromise Western systems.

Iran's leaders have described expansive plans to enhance their country's IT infrastructure, education, and training. Relaxing sanctions will allow them to accelerate and grow those plans even more. That will mean more resources to Iranian students and honest hardware and software developers, but also to malicious groups like Ashiyane and members of university faculties and research institutions that work closely with Iran's government and security forces.

For Iran, a cyberattack is a promising avenue by which Tehran could bring any future conflict to American soil.

If the Iranian regime appeared ready to embrace détente or peaceful coexistence with the West, and if it seemed ready to reduce its oppression of its own people, then it would be easy to argue for helping Iran develop its information economy. But Tehran continues categorically to reject either détente or any intention of loosening its grip on its own people. The US administration, moreover, appears to have rejected any notion of tying sanctions relief to either of those issues, focusing instead on nuclear nonproliferation goals.

It is difficult to imagine a future in which Iran does not become a significant cyberthreat to American national security. We must begin considering and shaping our response to that threat today. The current sanctions regime allows for a potentially much more rigorous policing of Western cyberinfrastructure to deny Iran the ability it now has to rent the most advanced computer systems from the West to use in attacking the West. It could also be tightened to further hinder Iran's ability to acquire and import advanced hardware and software with which to build its indigenous IT infrastructure. These options are lost, however, if the current sanctions regime is dismantled completely, a distinctly possible outcome of the nuclear framework agreement just concluded.

NOTES

1. Nart Villeneuve et al., "Operation Saffron Rose," webinar, FireEye, 2014, https://www2.fireeye.com/Operation-Saffron-Rose.html; Cylance, "Operation Cleaver," www.cylance.com/operation-cleaver/?gclid=CM_G5dXV4cQCFdcZgQodP7UAdw.

2. The framework agreement announces full relief from "nuclear-related" sanctions as soon as Iran complies with its commitments under the agreement—a process that should take months, but not years. The agreement is available at http://abcnews.go.com/Politics/wireStory/text-agreement-iran-nuclear-program-30079073.

3. Throughout this report, we use confidence assessments in accord with the standard intelligence community definitions. (See US Joint Chiefs of Staff, *Joint Intelligence*, October 22, 2013, https://fas.org/irp/doddir/dod/jp2_0.pdf.) Moderate confidence is defined as "partially corroborated information from good sources; several assumptions; mix of strong and weak inferences and methods; minimum intelligence gaps exist." We generally avoid assessing with "high confidence" because it is usually impossible to meet the standard of "well-corroborated information from proven sources," given the difficulty of obtaining cyberattack data relevant to any particular investigation from multiple reliable sources.

4. The US and the international community have been imposing sanctions on Iran for many years, long before the nuclear program was a major issue. See International Crisis Group, *Spider Web: The Making and Unmaking of Iran Sanctions*, Middle East Report No. 138, February 25, 2013, www.crisisgroup.org/~/media/Files/Middle%20East%20North%20Africa/Iran%20Gulf/Iran/138-spider-web-the-making-and-unmaking-of-iran-sanctions.pdf (particularly, www.crisisgroup.org/~/media/Files/Middle%20East%20North%20Africa/Iran%20Gulf/Iran/crisis-group-iran-sanctions-table.ashx) for a discussion of the complexity of sanctions in 2013. The recently announced framework for a nuclear deal will require careful examination and review before it is clear which sanctions will remain and which will go. See Frederick W. Kagan, "Complexities of Sanctions Relief," American Enterprise Institute, April 3, 2015, www.aei.org/publication/complexities-of-iranian-sanctions-relief/.

5. Kagan, "Complexities of Iranian Sanctions Relief."

6. "Executive Order—'Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities'," White House, April 1, 2015, https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

7. Jim Finkle and Rick Rothacker, "Exclusive: Iranian Hackers Target Bank of America, JPMorgan, Citi," Reuters, February 21, 2012, www.reuters.com/article/2012/09/21/us-iran-cyberattacks-idUSBRE88K12H20120921.

8. Ben Elgin and Michael Riley, "Now at the Sands Casino: An Iranian Hacker in Every Server," Bloomberg Business, December 11, 2014, www.bloomberg.com/bw/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas.

9. Philip Weiss, "Adelson Says Obama Should Fire 'Atomic Weapon' at Iran, Not Negotiate," Mondoweiss, October 23, 2013, http://mondoweiss.net/2013/10/adelson-nuclear-negotiate.

10. Christopher Bronk and Eneken Tikk-Ringas, "The Cyber Attack on Saudi Aramco," *Survival: Global Politics and Strategy* (April–May 2013): 81–96, www.iiss.org/en/publications/survival/sections/2013-94b0/survival--global-politics-and-strategy-april-may-2013-b2cc/55-2-08-bronk-and-tikk-ringas-e272.

11. Values calculated by averaging 10-day periods at the start of 2014 and mid-2015 to mitigate the effects of day-to-day variations.

12. Crossing disciplines increases the risk of miscommunication. "Open source" intelligence refers to publicly available (and therefore unclassified) information. The term "open source" has an entirely different meaning in the IT world, indicating program code that is not copyrighted and free for anyone to use.

13. The "dark web" is a portion of the Internet that is not readily visible to most users. It hosts a great deal of criminal activity, but it also hosts a lot of other things. A good basic discussion is found in Max Eddy, "Inside the Dark Web," *PC Magazine,* February 4, 2015, www.pcmag.com/article2/0,2817,2476003,00.asp.

14. "Siasat-haye kolli-ye 'eghtesad-e moghavemati'" [The Comprehensive Policies of 'Economy of Resistance'], Islamic Students News Agency, February 19, 2014, available in Persian at http://isna(.)ir/fa/news/92113020882/%D8%B3%DB%8C%D8%A7%D8%B3%D8%AA-%D9%87%D8%A7%DB%8C-%DA%A9%D9%84%DB%8C-%D8%A7%D9%82%D8%AA%D8%B5%D8%A7%D8%AF-%D9%85%D9%82%D8%A7%D9%88%D9%85%D8%AA%%8C-%D8%A7%D8

%A8%D9%84%D8%A7%D8%BA-%D8%B4%D8%AF; Amir Toumaj, *Iran's Economy of Resistance: Implications for Future Sanctions*, AEI Critical Threats Project, November 17, 2014, www.irantracker.org/analysis/toumaj-irans-resistance-economy-implications-for-sanctions-november-17-2014, 15.

15. Toumaj, *Iran's Economy of Resistance*, 16.

16. "World University Rankings, 2014–15," *Times Higher Education,* www.timeshighereducation.co.uk/world-university-rankings/2014-15/world-ranking/region/asia/range/001-200/order/country%7Casc.

17. United Nations, *E-Government Survey 2014: E-Government for the Future We Want*, 2014, http://unpan3.un.org/egovkb/Portals/egovkb/Documents/un/2014-Survey/E-Gov_Complete_Survey-2014.pdf.

18. See "Military Official Says 'Enemies' Try to Wage 'Soft War' against Iran," PressTV, December 4, 2008. For a detailed discussion of the concept, see "Iran Paper Warns of 'Enemy Infiltration, Soft War' against System, Revolution," BBC Monitoring Middle East, February 22, 2008.

19. "Khamenei: Iran in Throes of Soft War," Mail & Guardian, November 25, 2009, http://mg.co.za/article/2009-11-25-khamenei-iran-in-throes-of-soft-war.

20. "Soft War Headquarters to Develop Model for Confronting Enemy Soft Plots," Fars News Agency, January 26, 2013, www.thefreelibrary.com/Soft+War+Headquarters+to+Develop+Model+for+Confronting+Enemy+Soft...-a0316397013.

21. "Iran Planning to Set Up Provincial Soft War Headquarters," Fars News Agency, October 22, 2013, http://english(.)farsnews(.)com/newstext.aspx?nn=13920730001392.

22. Ali Akbar Dareini and Brian Murphy, "Iran Monitors Web in 'Soft War' with West," *Air Force Times*, April 16, 2012.

23. "Commander Calls for Concerted Efforts to Counter Soft War against Iran," Tasnim News Agency, January 11, 2014, www(.)tasnimnews(.)com/English/Home/Single/246507.

24. These ideas are pervasive in the writings and speeches of Khomeini. See, especially, "Islamic Government," reprinted in Ruhollah Khomeini, *Islam and Revolution: Writings and Declarations of Imam Khomeini (1941–1980)*, trans. Hamid Algar (North Haledon, NJ: Mizan Press, 1981), chapter 1, 27–39. This work derives from lectures given in Najaf, Iraq, in 1970, and focuses heavily on British influence: "The conspiracy worked out by the imperialist government of Britain at the beginning of the constitutional movement had two purposes. The first . . . was to eliminate the influence of Tsarist Russia in Iran, and the second was to take the laws of Islam out of force and operation by introducing Western laws." The anti-Americanism and anti-Zionism was clear even earlier: "All of our troubles today are caused by America and Israel. Israel itself derives from America; these deputies and ministers that have been imposed upon us derive from America—they are all agents of America, for if they were not, they would rise up in protest." See Ruhollah Khomeini, "The Granting of Capitulatory Rights to the US" (speech, Qom, Iraq, October 27, 1964), 25, 32, 187.

25. Richard Nixon, "Basic Principles of Relations between the United States of America and the Union of Soviet Socialist Republics," (speech, Moscow, Russia, May 29, 1972), www.presidency.ucsb.edu/ws/?pid=3438.

26. Ali Khamenei, Nowruz (New Year) Speech at the Imam Reza Shrine in Mashhad, Iran, March 21, 2015, http://farsi(.)khamenei(.)ir/speech-content?id=29236.

27. Warren Marshall, *Dispersed but Not Degraded: Iranian Universities and the Regime's Nuclear Weaponization Activities*, AEI Critical Threats Project, January 27, 2015, www.irantracker.org/nuclear/marshall-iranian-universities-and-nuclear-weaponization-january-27-2015.

28. "Dasturala'mal-e ertefa'-ye bahre-vari ez dure-ha-ye tahsilat-e takmili dar chaharchub-e tarh-e sarbazi bara-ye ta'min niaz-ha-ye keshvar" [Regulations to Improve the Usefulness of Graduate Courses in the Framework of a Military Service Plan to Secure the Needs of the Country], Armed Forces National Elite Foundation, March–April 2007, 3.

29. Christopher Rhoads and Loretta Chao, "Iran's Web Spying Aided by Western Technology: European Gear Used in Vast Effort to Monitor Communications," *Wall Street Journal*, June 22, 2009, www.wsj.com/articles/SB124562668777335653.

30. Craig Labovitz, "Iranian Traffic Engineering," Arbor Networks, June 17, 2009, www.arbornetworks.com/asert/2009/06/iranian-traffic-engineering.

31. Benjamin Elgin, Vernon Silver, and Alan Katz, "Iranian Police Seizing Dissidents Get Aid of Western Countries," Bloomberg,

October 30, 2011, www.bloomberg.com/news/articles/2011-10-31/iranian-police-seizing-dissidents-get-aid-of-western-companies.

32. International Atomic Energy Agency, Board of Governors, *Implementation of the NPT Safeguards Agreement and Relevant Provisions of Security Council Resolutions in the Islamic Republic of Iran*, November 2011, www.iaea.org/sites/default/files/gov2011-65.pdf.

33. "Blast Kills Commander at Iran Base," *New York Times*, November 13, 2011, www.nytimes.com/2011/11/14/world/middleeast/iran-blast-kills-revolutionary-guards-commander-at-base.html.

34. Rick Gladstone and Artin Afkhami, "Arrest of a Top Adviser to Iran's President Is Reported," *New York Times*, November 21, 2011, www.nytimes.com/2011/11/22/world/middleeast/ali-akbar-javanfekr-top-media-aide-of-iran-president-mahmoud-ahmadinejad-reported-held-in-raid.html; Robin Pomeroy, "Iranian Protesters Storm British Diplomatic Compounds," Reuters, November 29, 2011, www.reuters.com/article/2011/11/29/us-iran-britain-embassy-idUSTRE7AS0X720111129.

35. Collin Anderson, *Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran*, Annenberg School for Communication, Center for Global Communication Studies, June 2013, http://arxiv.org/pdf/1306.4361v1.pdf.

36. Ibid.

37. An autonomous system is one of a group of large servers that route data through the Internet. Autonomous systems are designated by numbers, so AS12880 or ASN 12880 is autonomous system number 12880.

38. As of April 3, 2015, AS 12880 originated 174 IPv4 prefixes including 2,207,746 IPs; AS 48159 originated 319 IPv4 prefixes but only 699,904 IPs; and AS 6736 originated only 8 IPv4 prefixes (and 2 IPv6 prefixes) with 131,328 IPs. Data from https://stat.ripe.net.

39. "Internet Filtering in Iran in 2004–2005: A Country Study," OpenNet Initiative, https://opennet.net/studies/iran; Rhoads and Chao, "Iran's Web Spying Aided by Western Technology."

40. "Iran, The Worl's [sic] Largest Cyber Army!" Hacker5, September 19, 2013, www(.)hackers5(.)com/iran-the-worls-largest-cyber-army.html (obtained from a Google cached copy as it appeared on March 3, 2015).

41. See Y. Mansharof, "Iran's Cyber War: Hackers in Service of the Regime," Middle East Media Research Institute, August 25, 2013, www.memri.org/report/en/print7371.htm. Mansharof cites a statement by Kamalian, but does not provide sufficient detail in the endnote to locate the statement.

42. Names and aliases for members of the Ashiyane team are posted on www(.)face2face(.)ga/index2.php. ActiveSpider does not appear on that list but gave his name (or alternate alias) as Ali Reza on the announcement of a Mac OS X exploit on May 17, 2005. See www(.)securiteam(.)com/exploits/5EP0D20FQC.html.

43. Mech(.)sharif(.)edu/~web/upload/center/def601474347.htm: "Defaced successfully, Behr00z_Ice, ActionSpider, r00t_b0x, Sha2ow, Azazel, [r00t_b0x@linuxmail.org], Ashiyane Digital Security Team w4z here… 07:45 p.m. 2008/jun/17; Happy Birthday To Me :) !"

44. "Council Implementing Regulation (EU) No 1002/2011 of 10 October 2011" *Official Journal of the European Union,* October 12, 2011, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:267:0001:0006:EN:PDF.

45. www(.)tabnak(.)ir/fa/news/196591/%D9%85%D8%B3%D8%A4%D9%88%D9%84%D8%A7%D9%86-%D8%A7%D8%B%8C%D8%B1%D8%A7%D9%86%DB%8C-%DA%A9%D9%87-%D8%A7%D8%AA%D8%AD%D8%A7%D8%AF%DB%8C%D9%87-%D8%A7%D8%B1%D9%88%D9%BE%D8%A7-%D8%AA%D8%AD%D8%B1%DB%8C%D9%85-%DA%A9%D8%B1%D8%AF (accessed April 3, 2015).

46. See "Iran, the Worl's Largest Cyber Army!"; and the "About Us" pages at ashiyane(.)org/aboutus.

47. The hacking group and the company are unquestionably tightly interwoven. The company website links to its forum at www(.)ashiyane(.)org, whose "About Us" page lists the hacker names of the Ashiyane hacking collective.

48. See, for example, "Certification," EC-Council, www.eccouncil.org/Certification/certified-ethical-hacker. There are indications that Kamalian and other members of Ashiyane may have received training based on materials and programs produced by the EC-Council. There are also accusations that EC-Council itself was involved in the training, which EC-Council denies. The denial generally appears as plausible as the accusation, given the ready availability of EC-Council materials, and the authors of this report take no position on this controversy. See Jeff Bardin, "Is This Gun Smoking? Certified Unethical Training," CSO, March 15, 2013,

www.csoonline.com/article/2136489/employee-protection/is-this-gun-smoking--certified-unethical-training.html.

49. See "Our Story," CloudFlare, www.cloudflare.com/our-story.

50. A "nameserver" is a particular kind of server system that translates a URL (domain name or website such as www.amazon.com) into an IP address (such as 192.168.1.24) that the Internet uses to route traffic. Nameservers are critical parts of the Internet and frequent targets for hackers. If a hacker can gain control of a nameserver, he can reroute all traffic aimed at a particular website to another website of his choosing, and only very careful and suspicious Internet users will notice.

51. See 7d(.)10(.)be(.)static(.)xlhost(.)com/English/main.php, accessed March 7, 2015. Al Manar's main URL, www(.)almanar(.)com(.)lb, resolves to 204.11.234.189, hosted by Vault Networks, which has data centers in Miami and Atlanta (www.vaultnetworks.com/facilities/miami-colocation, accessed April 3, 2015).

52. US Department of the Treasury, "US Designates Al-Manar as a Specially Designated Global Terrorist Entity Television Station Is Arm of Hizballah Terrorist Network," press release, March 23, 2006, www.treasury.gov/press-center/press-releases/Pages/js4134.aspx.

53. 24(.)le(.)be(.)static(.)xlhost.com/essaydetails.php?eid=561&cid=33 (accessed March 7, 2015).

54. www(.)al-akhbar(.)com/node/34648.

55. Ouriran(.)com/aboutus.cfm (accessed March 16, 2015).

56. See Amir Akhoundi Asl's LinkedIn page, https://www.linkedin.com/pub/amir-akhoundi-asl/73/3ab/432. The statement is under Asl's description of his role as technical manager.

57. See Ouriran(.)com/why.cfm (accessed March 16, 2015).

58. Reference available on request.

59. Reference available on request.

60. www(.)bankesoal(.)ir, www(.)bank-e-soal(.)ir, www(.)bank-keshavarzi(.)ir, ns1(.)bank-maskan(.)ir, www(.)banksoal(.)ir, www(.)gulfpetrochem(.)ir, www(.)keshavarzi-bank(.)ir, www(.)nanochelatingtechnology(.)ir, www(.)oilandgas(.)ir, www(.)parsethylene(.)ir, www(.)parsethylenekish(.)ir, www(.)parsethylene-kish(.)ir, www(.)petro-sahel(.)ir, mail(.)sabt(.)gov(.)ir, www(.)samin(.)ir, www(.)saminchemical(.)ir, tkdbank(.)ir, www(.)tkdbank(.)ir.

61. See the IRNIC list of resellers at www(.)nic(.)ir/List_of_Resellers, as of July 13, 2014.

62. Alireza Shirazi, interview by Shabnam Kohanchi, "Filtering Killed the Indicators of Blogosphere," Fanavaran, December 17, 2011, www.itmen.ir/index.aspx?pid=10324&articleid=3954.

63. Norse systems operate at an Internet layer low enough to detect IP spoofing (a practice by which hackers make it appear that their data is originating from a different IP address from the one that is actually generating it). We also rely on the results of Norse crawls of these IPs, which indicate servers do exist on them but that they are heavily firewalled or otherwise set up to reject crawling attempts.

64. Port 53 was open and responding as of April 5, 2015.

65. Mail(.)e-magine(.)co, resolves to this IP but is only a "coming soon" page.

66. John Leyden, "Gaping Network Port with Easy-To-Guess Password? You ARE the 79%," *The Register,* October 24, 2012, www.theregister.co.uk/2012/10/24/opportunistic_hackers/.

67. See Ali Alfoneh, "The Basij Resistance Force," http://iranprimer.usip.org/sites/iranprimer.usip.org/files/The%20Basij%20Resistance%20Force.pdf, for an excellent primer.

68. "Shahadat'eh javan ameli dar defai az harem ahul bayt + aks" [Martyrdom of Young Ameil Defending Ahlul Bayt Shrine + Photo], ABNA, March 25, 2015, available in Persian at www(.)abna24(.)com/persian/service/important/archive/2015/03/25/678946/story(.)html; "Shahadat'eh Mehdi Nowruzi dar defai az hareem mazhar Imameen Askareen + aks" [Martyrdom of Mehdi Nowruzi Defending Al-Askari Holy Shrine], ABNA, January 11, 2015, available in Persian at www(.)abna24(.)com/persian/service/middle/archive/2015/01/11/664059/story(.)html; "Akhareen madafeh irani karam imam hossein keh beh shahadah reseed + aks" [Latest Iranian Defender of the Imam Hossein Shrine Who Was Martyred + Photo], ABNA, December 10, 2014, available in Persian at www(.)abna24(.)com/persian/service/iran/archive/2014/11/10/650472/story(.)html; "Pekar shahid madafeh haram emrooz vared ilam me shavad" [Body of Martyr Defender of the Shrine Enters Ilam Today], *Ilam Bidar,* June 24, 2014, available in

Persian at http://ilamebidar(.)ir/news/8059.

69. Mohammad Nabi-Rudaki, "An Increase in Basij Missions," *E'temad-e Melli*, July 7, 2008, available from BBC Monitoring Middle East via World News Connection; Ali Alfoneh, "What Do Structural Changes in the Revolutionary Guards Mean?" AEI *Middle Eastern Outlook*, April 2009, www.aei.org/publication/what-do-structural-changes-in-the-revolutionary-guards-mean/.

70. US Department of State, "Department of Treasury and State Announce Sanctions of Iranian Security Forces for Human Rights Abuses," June 9, 2011, www.state.gov/r/pa/prs/ps/2011/06/165300.htm.

71. "Beh 2,000 basijis amouzesh vebblog nevisi dadeh me shavad" [2,000 Basijis Were Given Blog-Writing Training], Iran Green Voice, August 8, 2010, available in Persian at www(.)irangreenvoice(.)com/article/2010/sep/08/6918.

72. http://30mail(.)net/news/2010/nov/26/fri/5891 and www(.)farsnews(.)com/newstext.php?nn=13900829000784, summarized on Iran News Round Up, November 23, 2011, AEI Iran Tracker, www.irantracker.org/roundup/iran-news-round-november-23-2011.

73. http://basijpress(.)ir/fa/news-details/22672/%D9%86%D8%B8%D8%A7%D8%B1%D8%AA-%D8%B3%D8%AA%D8%A7%D8%AF%DB%8C-%D9%82%D8%B1%D8%A7%D8%B1%DA%AF%D8%A7%D9%87-%D9%81%D8%B6%D8%A7%DB%8C-%D9%85%D8%AC%D8%A7%D8%B2%DB%8C-%D8%B3%D9%BE%D8%A7%D9%87-%D8%AA%D9%87%D8%B1%D8%A7%D9%86-%D8%A7%D8%B2-%D9%86%D8%A7%D8%AD%DB%8C%D9%87-%D9%85%D9%82%D8%A7%D9%88%D9%85%D8%AA-%D8%A8%D8%B3%DB%8C%D8%AC-%D9%82%D8%AF%D8%B3/, summarized on Iran News Round Up, September 11, 2013, AEI Iran Tracker, www.irantracker.org/iran-news-round-september-11-2013.

74. Each of the websites identifies itself as "Corps of (unit eponym) of (province name) province," where "corps" is "*sepah*," which indicates something related to the IRGC (Sepah-e Pasdaran-e Enqelab-e Eslami—Corps of the Guards of the Islamic Revolution). The unit names correspond to units that Marie Donovan, analyst at the Critical Threats Project, has identified as belonging directly to the IRGC. (Donovan's report on the IRGC order of battle will be released in Summer 2015.) If the sites belonged simply to the Basij, they would have been titled something like "Basij of (province name)" without the distinctive "Sepah."

75. See, for example, the website of Fort Campbell, Kentucky, home of the 101st Airborne Division (Air Assault): www.campbell.army.mil/units/101st/Pages/default.aspx. It contains information about the history of the unit, status of base facilities, descriptions of subunits and their key leaders, information for new arrivals, access to military benefits, and so on. The IRGC websites are generally much more like polished local news outlets and do not provide detailed information about combat units or leaders except in the course of normal media reporting.

76. URLs include both province(.)basij(.)ir and sometimes www(.)province(.)basij(.)ir, which can sometimes lead to different IP addresses but do not in these cases.

77. West Azerbaijan Province is home to the Shohada Unit, which announced the migration of its website from azgh(.)basij(.)ir to sepahshohada(.)ir on December 6, 2014 (http://azgh(.)basij(.)ir/?q=node/14908. The site migration corresponded with a site redesign that brought the appearance and structure of the site in line with that of other provincial IRGC websites. Fars Province has the Fajr Unit and its website is tanvir(.)ir.

78. From the RIPE database: https://stat.ripe.net/AS50733#tabId=routing&routing_announced-prefixes.resource=AS50733&routing_announced-prefixes.starttime=2004-01-01T00:00 (accessed April 2, 2015).

79. "About Sharif University," www(.)sharif(.)ir/web/en (accessed March 23, 2015).

80. See also "Surprising Success of Iran's Universities," *Newsweek*, August 8, 2008, www.newsweek.com/surprising-success-irans-universities-87853.

81. See Sharif University website at www(.)sharif(.)ir/web/en/30 and Ce(.)sharif(.)ir/old/about/index.html.

82. Julian Taub, "Science and Sanctions: Nanotechnology in Iran," *Scientific American* Guest Blog, January 13, 2012, http://blogs.scientificamerican.com/guest-blog/2012/01/13/science-and-sanctions-nanotechnology-in-iran/.

83. Marshall, *Dispersed but Not Degraded.*

84. Office of Foreign Assets Control, "Non-Proliferation Designations; Non-Proliferation Designation Removals; Iran Designations," US Department of the Treasury, July 12, 2012, www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/

20120712.aspx.

85. Iran Watch, "Sharif University of Technology," Wisconsin Project on Nuclear Arms Control, December 9, 2014, www.iranwatch.org/iranian-entities/sharif-university-technology. See also Laurence Norman, "EU Loses Two New Iran, Syria Sanctions Legal Cases: EU General Court Demands More Detailed Evidence," *Wall Street Journal*, July 3, 2014, www.wsj.com/articles/eu-loses-two-new-iran-syria-sanctions-legal-cases-1404381644.

86. Office of Foreign Assets Control, "Update to the Iranian Financial Sanctions Regulations; Iran Sanctions Designations; Non-Proliferation Sanctions Designations; Anti-Terrorism Designations; Non-Proliferation Sanctions Designations Updates; Anti-Terrorism Sanctions Designations Updates," US Department of the Treasury, November 8, 2012, www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20121108.aspx.

87. Office of Public Affairs, "Fact Sheet: Sanctions on Iranian Government and Affiliates," US Department of the Treasury, n.d., www.treasury.gov/press-center/press-releases/Documents/Fact%20Sheet%20-%20Sanctions%20on%20Iranian%20Govt%20and%t20Affiliates%20-%20November%208,%202012.pdf.

88. See www(.)jalili(.)org (accessed March 23, 2015).

89. Ayasdi can also help visualize non-cyber data. Its initial use cases, in fact, were in the biomedical field. It relies on the application of Topological Data Analysis on top of standard clustering algorithms to produce its graphics. More information can be found at www.ayasdi.com/technology/.

90. Gibson Research Corporation, "Port 445," https://www.grc.com/port_445.htm.

91. "Conficker. Stop It, Block It," Symantec, April 13, 2009, www.symantec.com/connect/articles/conficker-stop-it-block-it.

92. "Windows Pass-Through Authentication Methods Improper Validation," Core Security advisory, March 10, 2015, www.coresecurity.com/advisories/windows-pass-through-authentication-methods-improper-validation. See also Common Vulnerabilities and Exposures, "CVE-2015-005," 2015, http://cve.mitre.org/cgi-bin/cvename.cgi?name=2015-0005; Microsoft Security Bulletin MS15-027, "Vulnerability in NETLOGON Could Allow Spoofing (3002657)," Microsoft Security TechCenter, March 16, 2015, https://technet.microsoft.com/library/security/ms15-027.

93. An excellent basic description of the process of firewalking can be found in David Irby, "Firewalk: Can Attackers See Through Your Firewall?" *SANS Global Information Assurance Certification Paper,* n.d., www.giac.org/paper/gsec/312/firewalk-attackers-firewall/100588.

94. Note that 89.165.0.14 by default resolves to 36.297N 59.6062E, a tiny town in the middle of nowhere west of Tehran. A Norse analyst located it in Tehran, at the DCI data center.

95. Toos-Ashena, or simply Ashena, is an ISP based in Mashhad. It is part of the Ashena Group, which appears to focus on providing IT services to Iranian universities, listing among its clients Tarbiat Modares, Elm-o-Sanat, Shahid Beheshti, Tehran, Mashhad Azad, Tehran Azad, and Payam-e Noor Universities; Mashhad and Semnan Medical Universities; and Iran Faragir Electronic Educational Institute. IP address 178.236.40.253, one of the main attackers, hosts one of the nameservers for Ashena(.)net. The other nameserver is hosted on 178.234.40.254. The only other systems visible in that network are a nameserver and mail server belonging to Varastegan Institute for Medical Sciences (on 178.236.40.240), which is also located in Mashhad (and, for some reason, not listed among Ashena Group's clients at www(.)ashena(.)net/en/index.php/clients, accessed March 18, 2015). IP address 89.165.0.14 shows a similar pattern. It hosted only a nameserver of Sabanet(.)ir, which is the ISP that owns this network and is the same as the Neda Gostar Saba Data Transfer Company (about which relatively little information is available). The other nameserver is hosted on 89.165.0.13, while sales(.)sabanet(.)ir is on 89.165.0.22. The only other infrastructure visible in this network are two nonfunctional URLs, ngsnet(.)net and www(.)pessyan(.)ir. Ngsnet is an abbreviation for Neda Gostar Saba.

96. The latter is more likely, at least in one case, because a ping of 89.165.0.14 (one of the attacking IPs) on March 18, 2015, succeeded. A DNS lookup that same day resolved ns2(.)ngsnet(.)net to 89.165.0.14 as well and found that ports 22 and 53 on that system were open, although ports 80, 8080, and 445 were closed. Pings of 178.236.40.253, however, failed. It appears that ns1(.)ashena(.)net has been moved to 178.236.39.253, which does respond to pings and has port 53 open. All of these IPs are behind Iran's firewall filter. Attempts to use a traceroute utility failed at the hop between the last AS outside of Iran and AS12880.

97. Karen Yourish and Josh Keller, "The Toll in Gaza and Israel, Day by Day," *New York Times*, July 15, 2014, www.nytimes.

com/interactive/2014/07/15/world/middleeast/toll-israel-gaza-conflict.html.

98. "To the Rescue? Muslim Hacktivists Prepare Cyber Retaliation against Operation 'Protective Edge'," SenseCy, July 9, 2014, http://blog.sensecy.com/2014/07/09/to-the-rescue-muslim-hacktivists-prepare-cyber-retaliation-against-operation-protective-edge/.

99. Gilad Zahavi, "#OpSaveGaza Campaign—Insight from the Recent Anti-Israeli Cyber Operation," SenseCy, August 11, 2014, http://blog.sensecy.com/2014/08/11/opsavegaza-campaign-insights-from-the-recent-anti-israel-cyber-operation/.

100. See Cylance, "Saffron Rose," for another discussion of Iranian attempts to compromise SCADA systems.

101. These IP addresses have another odd thing in common. Throughout 2014, several of them hosted nameservers for oddly named websites: brobackobama(.)com, broisenberg(.)com, and brolicopter(.)com (95.82.111.179 and 95.82.111.153, 95.82.99.109, and 95.82.104.98, respectively). The websites do not exist, and no record of them is found in the Wayback Machine. Searches on the names bring up references to possible gamer aliases, now disused, and an adorable YouTube video of a child attempting to pronounce the president's name.

102. Siemens Energy Inc., "Spectrum Power™ TG," 2010, http://w3.usa.siemens.com/smartgrid/us/en/transmission-grid/products/energy-management-and-scada-system-platforms/Documents/Spectrum-Power-TG-Overview-08-25-2010.pdf. The ports were 50020 and 50021 using UDP protocol from IPs 95.82.99.191, 95.82.104.126, and 95.82.104.98.

103. BBC News, "Iran 'Shoots Down Israeli Drone' Near Natanz Nuclear Site," BBC News, August 24, 2014, www.bbc.com/news/world-middle-east-28920361; "Implementation of the NPT Safeguards Agreement and Relevant Provisions of Security Council resolutions in the Islamic Republic of Iran," International Atomic Energy Agency, September 5, 2014, www.isis-online.org/uploads/isis-reports/documents/gov-2014-43.pdf.

104. Schneider Electric, "Telvent Infrastructure—OASyS Product Family Overview," www.schneider-electric.com/solutions/id/en/med/28715767/application/pdf/1623_oasys_family_prod_overview_usltr_2012.pdf.

105. Brian Krebs, "Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent," Krebs on Security, September 26, 2012, http://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/.

106. Kim Zetter, "Power Plants and Other Vital Systems Are Totally Exposed on the Internet," *Wired,* November 8, 2013, www.wired.com/2013/11/internet-exposed/.

107. Crawls six weeks after the attacks stopped briefly found a GoAhead Webserver application on the system, but subsequent crawls were either interrupted or failed.

108. Both CTP and the Institute for the Study of War have written extensively on the operations and methods of Iranian military, paramilitary, and proxy forces. See www.criticalthreats.org, www.irantracker.org, and www.understandingwar.org.

ACKNOWLEDGMENTS

Tommy Stiansen would like to acknowledge the invaluable contributions of the many expert analysts, editors, and engineers at Norse Corporation, without whom this report would have been impossible.

Frederick W. Kagan would like to thank a number of people for their contributions to this project. Heather Malacaria, program manager at CTP, was indispensable throughout this lengthy effort, developing innovative methods for conducting a great deal of open-source research rapidly and serving as a patient and devoted editor of many drafts. Marie Donovan and Mehrdad Moarefian, Iran analysts at CTP, were invaluable in collecting and translating Farsi-language materials as well as lending their insight. Zachary Scheinerman and other CTP interns were essential for their diligent collection and tagging efforts. Charlie Caris and Brett McCrae, along with one of our technology partners, Praescient Analytics, offered vital analytical support throughout this project. Harleen Ghambir, Heather Pickerall, and David Maxwell from the Institute for the Study of War also provided valuable assistance to this effort, for which we are very grateful.

ABOUT US

About the Authors

Frederick W. Kagan is the Christopher DeMuth Chair and director of the Critical Threats Project at AEI. In 2009, he served in Kabul, Afghanistan, as part of General Stanley McChrystal's strategic assessment team, and he returned to Afghanistan in 2010, 2011, and 2012 to conduct research for Generals David Petraeus and John Allen. In July 2011, Chairman of the Joint Chiefs of Staff Admiral Mike Mullen awarded him the Distinguished Public Service Award, the highest honor the chairman can present to civilians who do not work for the Department of Defense, for his volunteer service in Afghanistan. He is coauthor of the report *Defining Success in Afghanistan* (AEI and the Institute for the Study of War, 2010) and author of the *Choosing Victory* series of reports (AEI), which recommended and monitored the US military surge in Iraq. His most recent book is *Lessons for a Long War: How America Can Win on New Battlefields* (AEI Press, 2010, with Thomas Donnelly). Previously an associate professor of military history at West Point, Kagan is a contributing editor at the *Weekly Standard* and has written for *Foreign Affairs*, the *Wall Street Journal*, the *Washington Post*, the *Los Angeles Times*, and other periodicals.

Tommy Stiansen is the co-founder and chief technology officer of Norse Corporation. He is also the architect and inventor of DarkViking, the company's patent-pending technology and cloud security service. Stiansen began his IT career working for Scandinavian Airlines Systems as a technical team leader, responsible for air traffic operational challenges for the multinational airline. He then left to pursue entrepreneurial interests, launching some of the pioneering Internet companies in Norway. During this time Stiansen architected and built Charon, a telecommunications billing and operations support system software that was nominated for Most Innovative Product at the World Billing Awards in 2003. In 2004 he came to the United States to consult for several federal government agencies, including the Department of Homeland Security, and was chief architect of a "black box," utilized for national security and cyberwarfare scenarios, for a multinational corporation.

About AEI's Critical Threats Project

The Critical Threats Project of the American Enterprise Institute equips policymakers, opinion leaders, and the military and intelligence communities with detailed and objective open-source analysis of America's current and emerging national security challenges. Through daily monitoring, in-depth studies, graphic presentations, private briefings, and public events, the project is a unique resource for those who need to fully understand the nuance and scale of threats to America's security to effectively develop and execute policy.

About Norse Corporation

Norse is the global leader in live attack intelligence, helping companies block the threats that other systems miss. Serving the world's largest financial, government and technology organizations, Norse intelligence offerings dramatically improve the performance, catch rate, and return on investment of the entire security infrastructure. The Norse Intelligence Network, a globally distributed "distant early warning" grid of millions of sensors, honeypots, crawlers, and agents, delivers unmatched visibility into difficult-to-penetrate geographies and darknets, where bad actors operate. Norse processes hundreds of terabytes daily against a 7 petabyte attack history database, and weighs over 1,500 variables to compute real-time risk scores for millions of IP addresses and URLs every day.

About Our Technology Partners

The conclusions and assessments in this report do not reflect the positions of our technology partners.

AYASDI

Ayasdi is on a mission to make the world's complex data useful by automating and accelerating insight discovery. The company's Machine Intelligence software employs Topological Data Analysis, to simplify the extraction of knowledge from even the most complex data sets confronting organizations today—converting data into business impact.

ISW INSTITUTE FOR THE STUDY OF WAR

The Institute for the Study of War (ISW) advances an informed understanding of military affairs through reliable research, trusted analysis, and innovative education. ISW is committed to improving the nation's ability to execute military operations and respond to emerging threats in order to achieve US strategic objectives. ISW is a nonpartisan, nonprofit, public policy research organization.

NTREPID®

Ntrepid enables organizations to safely conduct their online activities. Ntrepid's Passages technology leverages the company's platform and 15-year history protecting the national security community from the world's most sophisticated opponents. From corporate identity management to secure browsing, Ntrepid products facilitate online research and data collection, and eliminate the threats that come with having a workforce connected to the Internet.

Palantir

Palantir Technologies is working to radically change how groups analyze information. We currently offer a suite of software applications for integrating, visualizing, and analyzing the world's information. We support many kinds of data including structured, unstructured, relational, temporal, and geospatial.

Præscient ANALYTICS

Praescient Analytics is a veteran-owned small business based in Alexandria, Virginia. Our aim is to revolutionize how the world understands information by empowering our customers with the latest analytic tools and methodologies. Currently, Praescient provides several critical services to our government and commercial clients.