The Future of Iranian Terror and Its Threat to the U.S. Homeland

Statement before the
House of Representatives Committee on Homeland Security
Subcommittee on Counterterrorism and Intelligence

Ilan Berman
Vice President, American Foreign Policy Council

February 11, 2016

Chairman King, Ranking Member Higgins, distinguished members of the Subcommittee:

It is an honor to appear before you today to discuss Iran's ongoing sponsorship of international terrorism and the impact that the new nuclear deal, formally known as the Joint Comprehensive Plan of Action (JCPOA), will have upon it. It is a topic that is of critical importance to the security of the United States and our allies abroad. While the Obama administration has argued that the signing of the JCPOA has enhanced both U.S. and global security, there is compelling evidence to the contrary: namely, that the passage of the agreement has ushered in a new and more challenging phase in U.S. Mideast policy.

SHORTFALLS OF THE JCPOA

While the JCPOA can be said to include some beneficial elements—including short-term constraints on Iranian uranium enrichment, a reduction in the number of centrifuges operated by the Islamic Republic, and a delay of the "plutonium track" of the regime's nuclear program—there is broad consensus among national security practitioners, military experts, scientists and analysts that the agreement is woefully deficient in several respects.

First, the new nuclear deal does not dismantle Iran's nuclear capability, as originally envisioned by the United States and its negotiating partners. Contrary to the White House's pledges at the outset of talks between Iran and the P5+1 nations in November 2013, the JCPOA does not irrevocably reduce Iran's nuclear potential. In

fact, it does the opposite; under key provisions of the JCPOA (specifically, those contained in Annex I, III and IV of the agreement[1]), the P5+1 nations have committed themselves to strengthening and reinforcing Iran's nuclear infrastructure and processes over the next ten years. As a result, the JCPOA enables a slower—but ultimately a stronger—Iranian nuclear program. When the agreement expires a decade from now, the Islamic Republic will be much closer to a breakout capability than it is today.

The new nuclear deal likewise incentivizes further proliferation, both on the part of Iran and by its neighbors. Although President Obama has claimed that the JCPOA closes off "all" of the pathways by which Iran can acquire a nuclear capability,[2] it focuses overwhelmingly on Iran's indigenous development—its domestic facilities, stockpiles and nuclear know-how. The agreement does not seriously address the parallel path by which Iran can acquire such a capability: the clandestine procurement of components from abroad.

This represents a serious oversight, because Iran maintains active proliferation relationships with a range of suppliers, including the regime of Kim Jong-un in North Korea and private commercial entities in the People's Republic of China. These sources have been essential to Iran's ballistic missile and nuclear advances to date, and can be expected to continue to provide technology and components that enable the Iranian regime to make progress on its nuclear effort in spite of heightened scrutiny over its domestic activities. Moreover, Iran's advances have nudged other countries in the Middle East—most conspicuously Saudi Arabia—to accelerate their own nuclear plans in response. As a result, there is significant potential for a destabilizing "proliferation cascade" in the region in coming years, and of the emergence of multiple nuclear aspirants along Iran's periphery.

Most significantly, however, the nuclear deal provides Iran with an economic windfall of unprecedented magnitude. As part of the terms of the JCPOA, the United States and its partners in the P5+1 agreed to release to Iran some $100 billion in previously escrowed oil revenue. As of this writing, Iran has full, unfettered access to these funds, without limitations on their use.

The scope of this economic stimulus is enormous. It amounts to roughly a quarter of Iran's annual GDP, which totaled $415 billion in 2014.[3] That sum rivals the entirety of the European Recovery Program (colloquially known as the Marshall Plan) launched by the Truman administration in 1948 in the aftermath of World War II—an initiative that disbursed $13 billion ($120 billion in today's dollars) to seventeen countries in Europe over the span of four years. The proportional impact of such relief for Iran is analogous to America's $16.7 trillion economy receiving an infusion of roughly $4.2 trillion—approximately five times the stimulus that stabilized the U.S. financial sector following the 2008 global economic crisis.

Moreover, these funds represent only one part of a considerably larger economic picture. While Iran's initial economic windfall will be at least somewhat dampened

by the declining global price of oil, the Iranian regime is adapting in response, including by revising its budget downward, focusing on non-oil exports, and significantly expanding domestic taxation.[4] Additionally, the economic stimulus enshrined in the JCPOA will invariably be augmented by the benefits of expanded post-sanctions trade between Iran and countries in Europe and Asia, many of which are now eagerly seeking economic reengagement with the Islamic Republic. This normalization, in turn, is being facilitated by Iran's reintegration into the global financial system via institutions from which it was previously proscribed, such as the Society for Worldwide Interbank Financial Telecommunications (SWIFT).[5]

As a result of these changes, the World Bank now estimates that Iranian GDP will grow by nearly 6 percent this year.[6] Simply put, the JCPOA has laid the groundwork for a sustained economic revival on the part of the Islamic Republic.

ANTICIPATING IRANIAN BEHAVIOR

How is Iran likely to use this economic windfall? The White House has argued that there is little reason for concern, because Iran can be expected to use the funds in question overwhelmingly for domestic reconstruction and economic stabilization,[7] and because the total sum available to Iran is considerably less than $100 billion as a result of the Islamic Republic's outstanding debts.[8]

This reasoning is deeply flawed. The U.S. government's estimate presupposes that the Iranian government will pay back all of its debts before accessing any of the previously-escrowed funds—an unrealistic prospect, particularly in light of the desire of creditor nations (such as China) to engage more deeply in trade with Iran now that sanctions have been lifted. Likewise, the Islamic Republic has a long and well-established history of preferring guns to butter. While some of the funds in question will undoubtedly be allocated for domestic projects, it is reasonable to expect that a portion—and perhaps a significant one—will be used by the regime on key strategic initiatives. These include:

Military modernization

The Islamic Republic is now poised for a period of sustained military expansion. On June 30th, 2015, two weeks before the formal conclusion of the JCPOA, Iranian Supreme Leader Ali Khamenei formally unveiled his government's Sixth Development Plan, which outlines an intention to expand the national defense budget by nearly $5 billion, to five percent of total GDP.[9] These plans are predicated upon Iran's ability to access additional resources as a result of the JCPOA and post-sanctions trade.

The Islamic Republic, moreover, is already beginning to move in this direction. In recent months, the Iranian regime has initiated new procurement talks for significant quantities of arms and materiel (including new aircraft, air defenses and battlefield components) with both Russia and China. Over time, such acquisitions will lead to a significant strengthening of Iran's ability to project power

into its immediate periphery, as well as its capacity to threaten and/or challenge its strategic rivals in the region, as well as American interests there.

Rogue state sponsorship

Although it has received comparatively little attention to date, one of the most significant consequences of the economic windfall inherent in the JCPOA will be its "trickle down" effect on the Islamic Republic's strategic partners. To date, Iran's relations with a host of revanchist and radical regimes—including Venezuela, Bolivia, Ecuador, North Korea, and Sudan, among others—have been constrained, at least in part, by a lack of resources. While Tehran maintains significant political, economic and military ties with all of those nations, bilateral contacts have been limited by Iran's own economic isolation, as well as by the financial weakness of these rogue state partners themselves.

This, however, may soon change. Given the scope of the sanctions relief contained in the JCPOA, Iran will shortly have the ability to strengthen those alliances significantly. Put simply, Iran has long served as a partner for an array of rogue states and repressive regimes globally. Today, however, Iran for the first time has the potential to serve as their patron—a position that will have pronounced negative effects on global security.

Terrorism financing

Back in 1984, the Reagan administration formally designated Iran as a state sponsor of terrorism for its involvement in, and orchestration of, the October 1983 attack on the U.S. Marine Barracks in Beirut, Lebanon. Today, the Islamic Republic still ranks as the world's foremost sponsor of international terrorism. As recently as this past summer, the Congressional Research Service estimated that the Islamic Republic spent between $3.5 billion to $16 billion annually on support for terrorism and insurgency worldwide.[10] That range encompasses:

- Extensive aid to the regime of Syrian dictator Bashar al-Assad (estimated at some $6 billion annually);
- Material and economic assistance to the Shi'a Houthi rebels in Yemen;
- Support for various Shi'a militias in Iraq;
- The entire operating budget of the Palestinian Islamic Jihad terrorist organization;
- Renewed aid (previously estimated at between $20-25 million monthly) to the Hamas terrorist group; and
- Between $100 and $200 million annually in financial support for Lebanon's Hezbollah militia.

These figures now have the potential to become much, much larger. White House officials have admitted that at least some of Iran's JCPOA-related economic windfall is likely to go to terrorist groups and extremist causes.[11] That, however, represents something of an understatement; given the size of the immediate sanctions relief at its disposal, should Iran allocate a mere 10 percent of its recently-unfrozen funds to such activities, it could double or even triple its current spending on terror sponsorship.

Regional expansionism

The past several years have seen the Islamic Republic embark upon an ambitious, multi-pronged effort to reshape the region in its own image. This effort has included, *inter alia*, attempts to undermine the monarchy in Bahrain; extensive backing for Yemen's Houthi insurgency; both financial and direct military assistance to the Assad regime in Syria, and; broad geopolitical support for Iraq's Shi'a militias. It has been animated by the Iranian leadership's conviction that, in the words of Iranian Supreme Leader Ali Khamenei himself, the international system is "in the process of change" and a "new order is being formed."[12] The message is unmistakable; Iran's leaders believe that declining Western influence provides their country with the opportunity to expand its reach and power in the Middle East.

The Iranian regime now has far greater ability to do so. Empowered by the resources inherent in the JCPOA, as well as the permissive political environment that has been created as a result, recent months have seen the Iranian regime adopt an increasingly expansionist foreign policy line. The consequences can be felt in deepening Iranian-Saudi tensions, multiple ballistic missile tests in violation of UN Security Council resolutions, and a more aggressive military posture in the Persian Gulf. These actions reflect the belief among Iranian policymakers, like Alaeddin Boroujerdi, chairman of the Iranian parliament's national security and foreign policy committee, that the security of the Persian Gulf is now "in Iran's hands."[13]

As the narrative above lays out, the expanded resources conferred by the JCPOA have the potential to dramatically increase the strategic capabilities of the Iranian regime—and, consequently, the threat it poses to international security. In the context of the United States homeland, these dangers are likely to be most pronounced in two distinct arenas.

AN EXPANDING FOOTPRINT IN LATIN AMERICA

The past decade has seen a systematic expansion of the Islamic Republic's strategic presence in the Americas. Using the sympathetic regime of Hugo Chavez in Venezuela as a gateway, Iran has dramatically broadened its diplomatic ties to the region, focusing in particular on the countries of the leftist political bloc known as the Bolivarian Alliance of the Americas (ALBA). Since 2005, Iran has nearly doubled the number of its embassies in the region, from six to eleven.[14] Its economic ties to the region have similarly ballooned, in particular its trade with the nations of Brazil, Bolivia and Ecuador.

This formal outreach has been mirrored by the establishment of a formidable asymmetric presence. Iran's informal activities in the region date back to the early 1980s, when it facilitated a foothold for its chief terrorist proxy, Hezbollah, in the so-called Tri-Border Region where Brazil, Argentina and Paraguay intersect. That presence, in turn, made possible the massive July 1994 bombing of the Argentine-Israel Mutual Association (AMIA) in Buenos Aires—an attack that Argentine state prosecutors subsequently concluded had been "ordered by the highest authorities of the Islamic Republic of Iran in conjunction with Hezbollah."[15]

Three decades on, Iran's asymmetric presence in the region is more extensive—and arguably far more lethal. As the late Argentine prosecutor Alberto Nisman detailed in his May 2013 indictment, over the past three decades Iran has successfully created a network of intelligence bases and covert centers in no fewer than eight Latin American countries: Brazil, Paraguay, Uruguay, Chile, Colombia, Guyana, Trinidad and Tobago, and Suriname.[16] This infrastructure has enabled Iran to initiate or support at least three separate plots against the U.S. homeland over the past decade.

- A 2007 plot involving Guyanese national Abdul Kadir to blow up fuel tanks underneath New York's John F. Kennedy Airport. According to Nisman, Kadir was a disciple and agent of Iranian cleric Mohsen Rabbani, the alleged mastermind of the 1994 AMIA bombing, and had previously "carried out the Iranian infiltration in Guyana" at Rabbani's direction.[17] Had it succeeded, the attempt would have caused "extensive damage to the airport and to the New York economy, as well as the loss of numerous lives," the FBI assessed.[18]

- An October 2011 attempt by Iran's Revolutionary Guard Corps (IRGC) to assassinate Saudi Arabia's ambassador to the United States at a DC restaurant, using members of Mexico's Los Zetas drug cartel to carry out the killing. In a press conference divulging details of the failed scheme, Attorney General Eric Holder noted that it was "directed and approved by elements of the Iranian government and, specifically, senior members of the Quds Force," the IRGC's elite paramilitary unit.[19]

- A plan by Venezuelan and Iranian diplomats to use Mexican hackers to penetrate U.S. defense, intelligence and nuclear facilities and launch widespread cyber attacks throughout the United States. The effort was detailed in a December 2011 investigative documentary by the Spanish-language TV network *Univision*, which featured audio recordings of the plotters, including a high-ranking Iranian diplomat.[20] In the wake of the documentary's airing, Venezuela's consul general to Miami was declared *persona non grata* and expelled from the country.[21]

Hezbollah's presence in the Americas has likewise continued to grow apace. Over the past several years, a string of incidents—among them the November 2014 apprehension of a Hezbollah operative in Lima, Peru; regional intelligence reports about Hezbollah activity in Mexico, Nicaragua, Chile, Colombia, Bolivia, and Ecuador; and revelations about official Venezuelan facilitation of the movement of Hezbollah operatives throughout the region via the provision of state-issued passports[22]—all point to a significant operational presence on the part of the terrorist group south of the U.S. border.

The risks to American security posed by this expanding footprint are both clear and present. Iran has already demonstrated both the capability and the intent to target the U.S. homeland, directly and via its proxies, through the Latin American theater. The capability for Iran to do so can be expected to grow in the near future. Given the priority attention that has been paid to Latin America by Iran in recent years, it is reasonable to expect that the Iranian regime will use its expanded resources to broaden and further solidify its footprint in the Western Hemisphere. If history is any judge, it will do so in a way that will be deeply inimical to American interests.

A MATURING CYBER ACTOR

Cyberspace is fast emerging as a new domain of conflict between Iran and the West. Beginning in the Fall of 2010, Iran's nuclear program was targeted by the Stuxnet computer worm, waking Iranian officials up to the fact that the West was attempting to compromise their nuclear effort. Subsequent attacks on Iranian nuclear facilities and infrastructure convinced Iran's leadership that cyber war had the potential to be—in the words of one top regime official—"more dangerous than a physical war."[23]

Iran mobilized in response. In July 2011, the regime formally launched an ambitious $1 billion governmental program to boost national cyber capabilities via the acquisition of new technologies, new investments in cyber defense, and the creation of a new cadre of cyber experts.[24] In tandem, it formed new, dedicated domestic agencies tasked with administering cyberspace, as well as creating a dedicated Cyber Defense Command within the Iranian military and an analogous Cyberspace Council in the *basij*, the country's repressive domestic militia.[25] Simultaneously, the Iranian government mobilized a "cyber army" of activists—nominally independent patriotic hackers (also known as "hacktivists") who have carried out attacks on sites and entities out of favor with the Iranian regime, including social networking platform Twitter, the Chinese search engine Baidu, and the websites of Iranian reformist elements.[26] The Intelligence Unit of Iran's clerical army, the Iranian Revolutionary Guard Corps (IRGC) allegedly oversees the activities of this "cyber army."[27]

Iran likewise has harnessed this growing capability against the West. The past several years have seen a range of aggressive—and increasingly capable—Iranian attacks on Western and allied interests via cyberspace.

- In the summer of 2012, Saudi Arabia's state oil giant, ARAMCO, was hit by an Iranian-developed virus called "Shamoon" that compromised three-quarters of the company's computers.[28]

- Between September 2012 and January 2013, multiple U.S. financial institutions (including Bank of America, JPMorgan Chase and Citigroup) experienced a series of distributed denial-of-service (DDoS) attacks that disrupted their online presence and functionality. Due to the sophistication

of the attacks, U.S. officials linked them definitively to the Iranian government.[29]

- In October 2013, the U.S. Navy's unclassified computer network was penetrated by hackers affiliated with the Iranian government, potentially compromising email and secure communications hosted on it.[30]

- In February 2014, the Nevada-based Sands Corporation experienced a computer attack that temporarily crippled its systems, an intrusion that has since been conclusively linked to Iran by the U.S. intelligence community.[31]

- In May 2014, cyber intelligence firm iSight Partners uncovered a complex Iranian "phishing" scheme dubbed "Newscaster," which was designed to compromise prominent political individuals of interest to the Islamic Republic through the use of social media.[32]

- In the spring of 2014, Iranian hacking group Ajax Security Team was found to have targeted U.S. defense firms with malicious software in order to gain access to their computers.[33]

- Iranian hackers are known to have extensively mapped U.S. infrastructure points, such as the power grid, trains, airlines and refineries, in what cyber experts fear could be a hostile contingency scenario in the event of a conflict with America.[34]

- Most recently, Iranian hackers carried out an extensive campaign of intelligence gathering aimed at the U.S. State Department in November 2015.[35] The effort included targeting diplomats with responsibility for Iran and the Middle East via both email and social media as part of what U.S. officials say is an increasingly aggressive attempt to glean information about American policies toward the Islamic Republic.

The scope of Iran's offensive cyber activities was outlined in detail in a December 2014 report by San Diego-based cybersecurity firm Cylance, which stated that: "Since at least 2012, Iranian actors have directly attacked, established persistence in, and extracted highly sensitive materials from the networks of government agencies and major critical infrastructure companies in the following countries: Canada, China, England, France, Germany, India, Israel, Kuwait, Mexico, Pakistan, Qatar, Saudi Arabia, South Korea, Turkey, United Arab Emirates, and the United States."[36] Targets of Iranian cyber attack identified by Cylance include oil and gas firms in Kuwait, Turkey, Qatar and France, aviation hubs in South Korea and Pakistan, energy and utilities companies in Canada and the U.S., and government agencies in the U.S., UAE and Qatar.

Moreover, the study suggests, this may represent merely the tip of the iceberg. "As Iran's cyber warfare capabilities continue to morph… the probability of an attack

that could impact the physical world at a national or global level is rapidly increasing," it concludes.[37]

Today, that warning is more salient than ever. Between 2014 and 2015, Iran—eager to reap the benefits of nuclear détente with the West—noticeably scaled back its online targeting of the West. But in the wake of this summer's nuclear deal, the Islamic Republic is ramping up its offensive cyber activities anew, for both political and strategic reasons. Domestically, Iran's hard-liners are at pains to assert their primacy in national affairs following the nuclear agreement—including over the regime's strategic programs, of which cyberspace is one. Abroad, Iranian leaders have increasingly come to see cyberspace as an indispensable domain for strategic influence, one that has risen in importance now that their country's nuclear program is at least temporarily constrained.

Given this emphasis, as well as the economic benefits of the JCPOA—which will increase the resources available to the regime to invest in its strategic capabilities—the Islamic Republic is poised to become an increasingly mature and formidable cyber power. In the process, it will invariably emerge as a serious cyber challenge for the United States.

LOOKING AHEAD

Since the start of nuclear diplomacy in November of 2013, the Obama administration has effectively downplayed the risks emanating from Iran. In its eagerness to conclude some sort of agreement with Iran over its nuclear program, the White House has systematically turned a blind eye to the Islamic Republic's fomentation of international terrorism, its support for rogue foreign regimes, and its strategic activities.

Now that implementation of the JCPOA has begun, Iran's capabilities in all of these areas have the potential to expand dramatically—and to do so to the detriment of American security. Tracking this growing destructive potential must become a top priority of the U.S. government. So, too, must the formulation of a strategy to identify, manage and limit Iranian rogue behavior in the years ahead.

---

[1] Annex I, Section H codifies Russia's commitment to cooperate with Iran on nuclear research at the Fordow Fuel Enrichment Plant. Annex III, Section D enshrines a European commitment to aid Iran in strengthening its nuclear security. Under Annex IV, Section 2, the P5+1 powers pledge to provide international assistance to Iran in mastering the nuclear fuel cycle through fuel fabrication.

[2] White House, Office of the Press Secretary, "Statement by the President on the Adoption of the Joint Comprehensive Plan of Action," October 18, 2015,

https://www.whitehouse.gov/the-press-office/2015/10/18/statement-president-adoption-joint-comprehensive-plan-action.

[3] "Iran GDP," Trading Economics, n.d., http://www.tradingeconomics.com/iran/gdp.

[4] "Iran's 2016 Budget Based on $35-40 Oil a Barrel," AzerNews, December 28, 2015, http://www.azernews.az/region/91180.html; "Next FY Budget Focuses on Foreign Capital, Non-Oil Exports," Mehr (Tehran), January 17, 2016, http://en.mehrnews.com/news/113637/Next-FY-budget-focuses-on-foreign-capital-non-oil-exports.

[5] "SWIFT to Restart Services to Iran by Jan. 31," *Tehran Times*, January 26, 2016, http://www.tehrantimes.com/index_View.asp?code=252493.

[6] "World Bank Forecasts 5.8% GDP Growth for Iran in 2016," *Tehran Times*, February 6, 2016, http://www.tehrantimes.com/index_View.asp?code=252783.

[7] Nadia Bilbassy-Charters, "Ben Rhodes: Iran's New Money Post Deal will Go to Uplift 'Terrible Economy,'" *Al Arabiya* (Riyadh), July 16, 2015, http://english.alarabiya.net/en/News/middle-east/2015/07/16/Ben-Rhodes-Iran-s-extra-revenue-after-nuke-deal-will-help-uplift-terrible-economy-.html.

[8] See, for example, "Lew: Iran Not Getting the Full $100 Billion of Frozen Assets," *The Fiscal Times*, July 26, 2015, http://www.thefiscaltimes.com/2015/07/26/Lew-Iran-Not-Getting-Full-100-Billion-Frozen-Assets.

[9] Abbas Qaidaari, "More Planes, Missiles and Warships for Iran," Al-Monitor, July 14, 2015, http://www.usnews.com/news/articles/2015/07/14/more-planes-missiles-and-warships-iran-increases-its-military-budget-by-a-third.

[10] Carla Humud, Christopher Blanchard, Jeremy Sharp and Jim Zanotti, "Iranian Assistance to Groups in Yemen, Iraq, Syria, and the Palestinian Territories," *Congressional Research Service Memorandum*, July 31, 2015, http://www.kirk.senate.gov/images/PDF/Iran%20Financial%20Support%20to%20Terrorists%20and%20Militants.pdf.

[11] See, for example, Matthew Lee, "Kerry: Some Iran Sanctions Relief Likely to Go to Terrorists," Associated Press, January 21, 2016, http://bigstory.ap.org/article/9ab669cada3b47cfaa3e6793a3ca6faa/kerry-rejects-iranian-criticism-us-sanctions.

[12] Arash Karami, "Ayatollah Khamenei Urges Iran to Prepare for 'New World Order,'" *Al-Monitor*, September 5, 2014, http://www.al-monitor.com/pulse/originals/2014/09/khamenei-new-world-order.html#.

[13] "Persian Gulf Security in Iran's Hands: Senior MP," Tasnim (Tehran), January 14, 2016, http://www.tasnimnews.com/en/news/2016/01/14/971145/persian-gulf-security-in-iran-s-hands-senior-mp.

[14] Iran today boasts an official diplomatic presence in Argentina, Bolivia, Brazil, Chile, Colombia, Cuba, Ecuador, Mexico, Nicaragua, Uruguay and Venezuela.

[15] Marcelo Martinez Burgos and Alberto Nisman, "AMIA Case," Investigations Unit of the Office of the Attorney General, 2006, http://www.peaceandtolerance.org/docs/nismanindict.pdf.

[16] Guido Nejamkis, "Iran Set Up Terrorist Networks in Latin America: Argentine Prosecutor," Reuters, May 29, 2013, http://www.reuters.com/article/2013/05/29/us-argentina-iran-idUSBRE94S1F420130529.

[17] Ibid.

[18] Federal Bureau of Investigation, New York Field Office, "Abdul Kadir Sentenced to Life in Prison for Conspiring to Commit Terrorist Attack at JFK Airport," December 15, 2010, http://www.fbi.gov/newyork/press-releases/2010/nyfo121510a.htm.

[19] Charles Savage and Scott Shane, "Iranians Accused of a Plot to Kill Saudis' U.S. Envoy," *New York Times*, October 11, 2011, http://www.nytimes.com/2011/10/12/us/us-accuses-iranians-of-plotting-to-kill-saudi-envoy.html?pagewanted=all.
[20] "La Amenaza Irani," *Univision*, December 9, 2011, http://noticias.univision.com/article/786870/2011-12-09/documentales/la-amenaza-irani/la-amenaza-irani.
[21] "U.S. Expels Venezuelan Diplomat in Miami," CNN, January 9, 2014, http://www.cnn.com/2012/01/08/us/venezuela-consul/.
[22] Barak Ravid, "Hezbollah Member Held in Peru for Planning Terror Attack," *Ha'aretz* (Tel Aviv), October 30, 2014, http://www.haaretz.com/world-news/.premium-1.623743; "Latin America Takes Action to Control Hezbollah's Activities," *Asharq Al-Awsat* (London), January 25, 2016, http://english.aawsat.com/2016/01/article55346877/latin-america-takes-action-to-control-hezbollahs-activities; "Venezuela Exposes the Involvement of Hezbollah and Iran in the Americas," *Janubia*, January 27, 2016, http://janoubia.com/2016/01/27/أفـي-واي-ران-الله-حزب-تورّط-تفـضح-فـنزويلا/.
[23] "Iran Sees Cyber Attacks as Greater Threat than Actual War," Reuters, September 25, 2012, http://www.reuters.com/article/2012/09/25/net-us-iran-military-idUSBRE88O0MY20120925.
[24] Yaakov Katz, "Iran Embarks On $1b. Cyber-Warfare Program," *Jerusalem Post*, December 18, 2011, http://www.jpost.com/Defense/Article.aspx?id=249864http://www.jpost.com/Defense/Article.aspx?id=249864.
[25] See, for example, Kevjn Lim, "Iran's Cyber Posture," *OpenBriefing*, November 18, 2013, http://www.openbriefing.org/regionaldesks/middleeast/irans-cyber-posture/.
[26] Farvartish Rezvaniyeh, "Pulling the Strings of the Net: Iran's Cyber Army," PBS *Frontline*, February 26, 2010, http://www.pbs.org/wgbh/pages/frontline/tehranbureau/2010/02/pulling-the-strings-of-the-net-irans-cyber-army.html; Alex Lukich, "The Iranian Cyber Army," Center for Strategic & International Studies, July 12, 2011, http://csis.org/blog/iranian-cyber-army.
[27] University of Pennsylvania, Annenberg School of Communications, Iran Media Program, "Internet Censorship in Iran," n.d., http://iranmediaresearch.org/sites/default/files/research/pdf/1363180689/1385/internet_censorship_in_iran.pdf.
[28] Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *New York Times*, October 23, 2012, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all.
[29] Nicole Perlroth and Quentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say," *New York Times*, January 8, 2013, http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?pagewanted=1&_r=0.
[30] Julian E. Barnes and Siobhan Gorman, "U.S. Says Iran Hacked Navy Computers," *Wall Street Journal*, September 27, 2013, http://www.wsj.com/articles/SB10001424052702304526204579101602356751772.
[31] Tony Capaccio, David Lerman and Chris Strohm, "Iran Behind Cyber-Attack on Adelson's Sands Corp., Clapper Says," Bloomberg, February 26, 2015, http://www.bloomberg.com/news/articles/2015-02-26/iran-behind-cyber-attack-on-adelson-s-sands-corp-clapper-says.

[32] Mike Lennon, "Iranian Hackers Targeted US Officials in Elaborate Social Media Attack Operation," *Security Week*, May 29, 2014, http://www.securityweek.com/iranian-hackers-targeted-us-officials-elaborate-social-media-attack-operation.
[33] Dune Lawrence, "Iranian Hackers, Getting More Sophisticated, Target U.S. Defense Companies," Bloomberg, May 14, 2014, http://www.bloomberg.com/bw/articles/2014-05-14/iranian-hackers-getting-more-sophisticated-target-u-dot-s-dot-defense-companies.
[34] Brian Ross, "What Will Happen to the US if Israel Attacks Iran?" *ABC News*, March 5, 2012, http://abcnews.go.com/Blotter/israel-attacks-iran-gas-prices-cyberwar-terror-threat/story?id=15848522#.T4g5tqvY9Ll.
[35] David E. Sanger and Nicole Perlroth, "Iranian Hackers Attack State Dept. via Social Media Accounts," *New York Times*, November 24, 2015, http://www.nytimes.com/2015/11/25/world/middleeast/iran-hackers-cyberespionage-state-department-social-media.html.
[36] Cylance, *Operation Cleaver*, December 2, 2014, http://www.cylance.com/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf.
[37] Ibid.