What Does Iran's Cyber Capability Mean For Future Conflict?

by James P. Farwell and Darby Arakelian

The saber rattling rhetoric of Iranian President Mahmoud Ahmadinejad has fueled fears that Iranian-driven Shia politics may polarize the region and spark conflict or civil strife.[1] Israel remains notably unsettled by Iran's nuclear program and Ahmadinejad's belligerent public remarks, floating rumors of a 30-day war with Iran.[2] Ironically, Ahmadinejad lacks the power to act on such rhetoric, as control over Iran's military resides with its Supreme Leader Ayatollah Ali Khamanei.

In light of these regional tensions, what is the emerging strategic reality vis-à-vis Iran? In the policy sphere there exists a debate over whether a pan-Shiism unified leadership may destabilize the region or whether the more pressing challenge lies in containing Iranian efforts to assert strategic and cultural hegemony in the region.

This paper focuses more on the strategic considerations and role of Iran's cyber capability in regards to regional instability and future conflict. There are offensive and defensive aspects to that strategic equation, which must be understood and addressed. Iran has shown a willingness to employ cyber tools to maintain the power of the regime at home as well, it appears, to influence the policies or posture of other nations towards Iran in order to deter cyber attacks or other action that Iran deems hostile to its interests.

We believe that Iran will pursue an aggressive regional policy that employs cyber tools that affect its neighbors and the West. These tools include malware that can disable critical infrastructure, create confusion, distrust, deception, disruption, support or to drive psychological operations that deter hostile activity or otherwise achieve strategic or tactical objectives. Weapons like Stuxnet offer the threat of cyber weapons without tying them to a particular strategic need or a state's capacity to mount operations. The tools may offer particular value in complementing kinetic strategies and tactics.

James P. Farwell is an attorney, an expert in cyber strategy and strategic communication, and has advised the U.S. Department of Defense. He is the author of *The Pakistan Cauldron: Conspiracy, Assassination & Instability* (Washington: Potomac Books, 2011) and *Persuasion and Power*, to be published by Georgetown University Press in November.

Darby Arakelian, a former officer with the Central Intelligence Agency, is a U.S. Government contractor consulting on global traditional and social media insights and trends. The views expressed are those of the authors and do not represent the views of the U.S. Government, or any of its departments, agencies, or COCOM.

Iran seems likely to take steps that increase or leverage its influence among Shia populations. Iran will not likely voluntarily relinquish development of its nuclear arms program. It will try move to strengthen military and economic ties with Russia, China, and India, and try to manipulate those relationships to evade or minimize the impact of international sanctions.

Until Iran has improved its cyber offensive and shored up its defensive capabilities, it seems unlikely to engage in a near-term regional conflict. To fortify its hold on power at home, the ruling regime must strengthen its ability to withstand kinetic cyber attacks. Offensive cyber capabilities are equally important since they enable Iran to exert influence that may, at a minimum, keep its perceived adversaries off balance and potentially de-stabilize their internal political dynamics.

Iran Strengthens Its Cyber Capabilities

Understanding the cyber capabilities Iran finds necessary for regime survival requires examining the challenges Iran confronts at home from dissenters, evaluating Iran's need to strengthen its external defensive capabilities, and examining the role that cyber technology plays in both quelling dissent and providing external security. Such analysis highlights possible offensive tools that could help Iran achieve its political objectives. Already Iran has shown an aggressive posture in building and employing cyber tools. Forging an effective offensive strategy requires clear comprehension of the weaknesses that render a state vulnerable. For Iran, identifying these weaknesses will help the country anticipate and establish plausible responses to cyber attack or cyber exploitation (espionage).

Response development is crucial for operating in today's new era of asymmetric conflict, as the political nature of warfare, rather than its kinetics, may be paramount. While warfare will always entail efforts to destroy an enemy, it may be better strategy to focus on the narrower goal of paralyzing an enemy's command and control, or neutralizing an adversary's ability to achieve its own goals through disruption, destruction, confusion, deception, and distrust. Cyber tools offer alternative means of achieving these goals, including the ability to administer operational shock and other psychological effects. However, elevating employment of cyber malware to the status of "use of force" can quickly trigger escalatory responses, ruinous to states engaged in such conflict.

Cyber tools offer a different and arguably easier route to negatively impacting the economy of another state. They offer the added advantage of allowing a hostile state to operate anonymously. One of the great challenges in defending against cyber attacks lies in the problem of identifying an attacker, especially where the party may operate through a third-party proxy. The Law of Armed Conflict renders identification essential in ensuring proportional response to a cyber attack and to avoid inflicting collateral damage to innocent parties, especially civilians.[3] Iran's experience in fighting internal dissent illustrates how cyber tools may be employed for offense or defense. Understanding how Iran manipulates its cyber tools is vital to the creation of security policies that can anticipate and counter any future actions

Iran may take to undercut the security interests of the U.S. and its allies.

Stuxnet and Other Malware

The Stuxnet computer worm served as a wake-up call to Iran. Iranians were shocked at the June 2010 discovery of the worm—a form of computer malware—which struck the Iranian nuclear facility at Natanz.[4] Computer World called it "one of the most sophisticated and unusual pieces of software ever created."[5] New York Times reporter David Sanger reported that the attack caught Iranians flat-footed. They had no idea what was happening even while the cyber attack was in progress.[6] Reportedly created by the U.S. and Israel, Stuxnet's damage on Iran's nuclear centrifuges remains unclear.[7] Estimates suggest that it damaged twenty-five to thirty percent of centrifuges and set back the Iranian nuclear program by several years. Iran reported that about 1,000 centrifuges were decommissioned and replaced and perhaps 11 of 18 cascades (each containing 164 centrifuges) were disconnected.[8]

THE USE OF STUXNET MALWARE ALSO RAISED COMPLEX ISSUES REGARDING WHETHER THE CYBER ATTACK COULD BE CLASSIFIED AS A "USE OF FORCE"

Despite admitting the attack and blaming enemies of Iran, Ahmadinejad was vague about the actual damage: "They succeeded in creating problems for a limited number of our centrifuges with software they had inserted in electronic parts," he told the media. "Fortunately our experts discovered that and today they are not able [to do that] anymore."[9] The use of Stuxnet malware also raised complex issues regarding whether the cyber attack could be classified as a "use of force," within the meaning of United Nations Article 2(4), whether it fell within the ambit defense against "armed attack" under Article 51, or whether it constituted an Act of War.[10]

Iran had several response options, but chose to play down the incident. Its strategic communications articulated the messages that little damage had been inflicted, nothing would deter Iran from moving forward to pursue its national interests, and Iranians should not become unduly alarmed. Actually, one can reasonably presume that Iran's national security team was far more concerned than they let on. Many believe that Iran intended to send a message that it will respond aggressively to the use of malware such as Stuxnet that targeted Iran. They point to the Shamoon malware attack that hit Saudi Aramaco in September 2012, damaging perhaps 30,000 workstations as a specific response to the Stuxnet attacks.[11] Iran drew credit for an attack on Qatar-based RasGas that inflicted a major malware infection.[12] U.S. officials have suggested that Iran was also the culprit behind attacks on large American banks such as Capital One Financial Corp. and BB&T Corp.[13]

These developments may signal the emergence of a new era in which cyber engagements may or may not rise to the level of use of force, armed attack, or war, but that seek to achieve specific strategic or tactical effects that influence the behavior of adversarial States. Stuxnet, which Sanger reported evolved in different

iterations, was just the opening gun in a series of cyber attacks against Iran. The espionage tool Flame, apparently twenty times more powerful than Stuxnet, was just one of several viruses that infiltrated Iranian cyber infrastructure to gather intelligence, operating by logging keyboard strokes, recording conversations by activating microphones, and taking screen shots.[14] The viruses dubbed Duqu, Madi and Gauss also revealed Iranian vulnerability to cyber-exploitation—techno-speak jargon for cyber espionage.

IRAN'S CAPABILITIES MAY BE LESS POWERFUL THAN THOSE OF THE U.S., CHINA, OR RUSSIA, BUT IT WOULD BE A MISTAKE TO IGNORE THEIR EXISTENCE AND DEVELOPMENT.

Labeled "quite unsophisticated," by Alexander Gostev, chief security expert of the Kaspersky Lab in Russia, Madi nevertheless "enabled the attackers to infect the high-profile victims who were tricked with social engineering schemes. No advanced exploit techniques or zero-days are used anywhere in the malware, which makes the overall success of the campaign very surprising to experts."[15] Apparently Madi delivered a malicious Trojan through social engineering schemes which enabled it to steal files from infected Windows computers, monitor email and instant messages, record audio, log keystrokes, and take screenshots of victims' activities. The Russian cyber company Kaspersky Lab, and Seculert, reported that Madi struck at accounts on Gmail, Hotmail, Yahoo!, Mail, ICQ, Skype, Google+ and Facebook.[16]

Gostev points out that Gauss resembled Flame in design and code base, although its aim differed. Unlike Flame, Gauss targeted lots of users in select countries to steal banking and financial information. Although Iran has remained silent, Kaspersky Lab has identified Iran—along with Israeli and other Middle East parties—as intended targets. Additionally, Iran has confirmed that Duqu, another virus, was detected within its cyber infrastructure.[17]

Not all attacks on Iranian cyber defenses have inflicted damage or stolen data. In July 2012, news surfaced that a virus had attacked an Iranian atomic research facility's air conditioning and blasted AC/DC rock-and-roll music.[18] While its effects were rather trivial, this case further illustrates Iran's weaknesses in its cyber defenses. Center for Strategic & International Studies (CSIS) cyber expert Alex Lukich bluntly concluded that Iran's cyber capabilities are "inferior."[19]

Using Cyber Tools to Repress Dissent

Iran's capabilities may be less powerful than those of the U.S., China, or Russia, but it would be a mistake to ignore their existence and development. Iran has embarked upon a $1 billion cyber program to boost its capabilities: developing new technology, hiring experts, and moving swiftly towards a centralized filtering system.[20] Iran created an Iranian Cyber Army (ICA) reportedly to hack into government and business websites to generate international awareness of its presence. It is unclear whether the ICA consists of Iranians or includes (or actually

consists of) Russians.[21] Ebrahim Jabbari, head of Iranian Revolutionary Guard Corp's (IRGC) Ali Ebn-e Abitaleb Corps in Qom, claims that the IRGC has set up the second-biggest cyber army in the world.[22]

Iran understands and can execute hacking. Google executive Eric Schmidt expressed high admiration for Iranian ability, stating "Iranians are unusually talented [at cyber warfare] for some reason we don't fully understand" when referring to the Iranian infiltration of Danish cyberspace.[23] Iranians penetrated Dutch websites by hacking into the Diginotar computer system, a Dutch government site that issues security certificates. Currently, Iranian agents have hacked into 500 certifications. Iran may have also hacked into the control system of the unmanned US drone it recently captured.[24]

The Iranian regime's ability to conduct effective blocking and surveillance tactics against dissidents was evident during the Green Revolution, commonly referred to as "Iran's Twitter Revolution." Triggered by cries of election fraud after the 2009 Presidential election, in which Ahmadinejad claimed victory over Mousavi, protestors used Twitter and social-networking sites to rally support against the regime.[25] With its high literacy rates and wide Internet use, Iranian protestors effectively leveraged e-mail, YouTube, Twitter, Facebook, and other sites to communicate and upload videos of demonstrations and regime violence. Tweets communicated real-time accounts of what was happening.[26] Cyber tools enabled demonstrators to forge an identity of opposition and to engage effectively in places like Tehran's Freedom Square. In conjunction with their social networking efforts, protestors initiated Distributed Denial of Service (DDoS) attacks against government websites.[27]

Although the regime clamped down by blocking internet communication through its own DDoS attacks,[28] banning international journalists from covering rallies,[29] and shutting down Al Arabiya offices in Tehran,[30] the dissent reignited in 2011. To maintain governmental censorship, Iran routes its Internet traffic through the government-run company Data Communication of Iran (DCI). DCI can program its Internet routers to block access to sites, like YouTube or Facebook, shut off the Internet, or to provide slow service.[31] The 2011 protestors countered DCI control by using proxy sites outside Iran to bypass government censors.

The evasion of governmental controls is a fast-moving game of cat-and-mouse. As quickly as the government identifies and shuts down sites, protestors move to new sites that are pushed out to them. The New York Times cited the videoed death of Neda Agha-Soltan as an example of successful Iranian evasion of government Internet controls. Dodging censors who shut down YouTube and Facebook, the videographer of Agha-Soltan's death got the 40-second video to the Voice of America and London's The Guardian. The video went viral and in this instance the Iranian regime proved ineffective at silencing dissent.

During the 2011 protests,[32] digital communication among protestors using Twitter, Facebook, Flickr, YouTube and proxy sites fueled activism. The regime reacted, shutting down opposition leader Mir Hossein Mousavi's website,[33]

disrupting text-message and mobile phone service, and blocking news sites and bahman, the Persian word for calendar, from the Internet. The regime also jammed TV broadcasts and prohibited photography.[34]

As protests spread across the region, regime was determined to clamp down on any activity that threatened regime stability. Tehran's deputy public prosecutor, Mahmoud Salarkia, announced that "a special court to examine electronic and computer-related crimes will be established." The IRGC weekly, Sobh-e Sadeq, warned against "Internet imperialism" and the danger of a "velvet Internet revolution" conspiring to overthrow the regime.[35] The Iranian Supreme Council of Virtual Peace, which provides guidance to police, communicated the need to protect Iranians from "immoral material" while criticizing the U.S. for waging a "soft war" against Iran through online aggression.[36]

Skeptics like Evgeny Morozov[37] argue that those who see the Internet as inevitably producing democracy or accountable government by mobilizing populations against authoritarian rule through social networking are too optimistic. The Mullahs made arrests and staged their own version of Stalinist show-trials, and what "seemed like Leipzig in 1989 was beginning to resemble Beijing of that same year."[38] Morozov notes that despite Iran's population of 70 million, before the protests, it had less than 20,000 Twitter users. The "protests that engulfed the streets of Tehran were not spontaneous or 'flash-mobs,'" he argues, but part of a carefully planned and executed strategy by the Mousavi camp.[39] He contends that the opposition was well organized, expected election fraud, and prepared to take action. In his view:

> *A Twitter Revolution is only possible in a regime where the state apparatus is completely ignorant of the Internet and has no virtual presence of its own. However, most authoritarian states are now moving in the opposite direction, eagerly exploiting cyberspace for their own strategic purposes….As it happens, both Twitter and Facebook gave Iran's secret services superb platforms for gathering open source intelligence about future revolutionaries, revealing how they are connected to each other.*[40]

Disdainful of external support for the dissenters, he points out that their attacks caused the state to slow down the entire Iranian Internet, "making it difficult to obtain any (even non-government) information or upload photos or videos from the protests. Thus, foreigner supporters managed to do what the Iranian government could not: make the Internet unusable for activists."[41]

Morozov raises valid considerations, and if one views Twitter as a stand-alone channel for igniting and sustaining a revolution, he makes a powerful point. However, Twitter is not the only outlet for the circumvention of regime control. Dissenters employed Twitter in tandem with other cyber communication tools, including Facebook, YouTube, broadcast, email, and text messaging.

In Syria, cyber tools have proven vital for recruiting, mobilizing, and

coordinating rebel activity against the regime of Syrian President Bashar al-Assad. Assad has employed the same sophisticated tools of blocking, control, and surveillance of cyber communication as the Mullahs in Tehran. The difference between Iran and Syria so far has been that Syrians have been willing and able to incite and sustain a violent civil war. Cyber technologies have played a key role in the conflict, but they represent only one aspect of the dynamics that drive the realities on the ground.

Iranian Cyber Capacity Building

Iran is building capacity through several confluent approaches. These include developing a trained cyber force, leveraging alliances, and mobilizing the considerable talent of Iranians in the cyber field. Iranians, as a culture, are proud of their talent for science and mathematics; their country is a large, highly literate, well-educated nation. One should expect it to possess a talented pool from which to forge a top-tier cyber capability. Iran may be a U.S. adversary and provides poor governance, but it has shown a gift for mischief.

Jabbari claimed that the IRGC has set up the second-biggest cyber army in the world.[42] The ICA is the best known—or, depending upon one's perspective, notorious—Iranian cyber force, whose activities have increasingly drawn international notice and are closely linked to the regime. The scope of ICA's actions includes hacking sites and issuing warnings to the Green Movement. In December 2009, it attacked Twitter; a year later, it hacked Baidu, China's largest search engine, triggering a series of cyber engagements between China and Iran. In February 2012, the ICA hacked Jaras News, a source which reports on the Green Movement, placing a message denouncing Jaras News as tool of America.[43] It has hacked Farsi 1, a site accused of being anti-Islamic.[44] ICA targets have also included the Voice of America and its ninety-five affiliated websites, on which the ICA placed a billboard displaying an Iranian flag and a gun complete with the declaration: "We have proven that we can."[45]

Attacking websites is just one of ICA's tactics. Computerworld reports that ICA claims the attack on TechCrunch's European website, and the installation of a page on TechCruch's site that redirected visitors to a server which attempted to install malicious software on visitors' PCs. Security startup Seculert asserts that ICA may be running a botnet – a network of Internet-connected computers whose security defenses have been breached and control usurped by a malicious party. That conclusion is based on similarities in the e-mail address of the group that defaced Twitter and Baidu sites. However, whether Seculert is correct has been debated. Reuters reported there is no certainty either attack came from an Iranian group.[46] Cyber expert Jim Lewis of CSIS is also dubious: "This is ham-handed so it's probably not the Iranian government. It could be sympathizers."[47] Still, Seculert believes the botnet has infected as many as 20 million PCs, distributing malicious software, such as Zeus, used to hack into online banking accounts, and data-stealing Trojans, like Gozi and Carberp.[48]

Recruiting is a ruthless process in Iran's cyber world. Targeted recruits are given a choice: join or jail. Brig. Gen. Gholamreza Jalali, who leads Iran's Passive Defense Organization, has declared that Iran plans "to fight our enemies with abundant power in cyberspace and internet warfare" by recruiting highly paid hackers.[49] The technical ability of members is rated as comparable to American and Israeli intelligence operatives, although there is no reason to believe that Iran's cyber capability matches that of the U.S. or Israel. Other groups have included Ashiyaneh, Shabgard, and Simorgh. Ashiyaneh reportedly includes skilled hackers and is the most widely recognized.[50] Members of Ashiyaneh wasted little time in "wrecking the sites of the Islamic Republic's opponents," and reports of their activities have been published in Iranian government media.[51] Supreme National Security Council General Secretary Saeed Jalili has claimed that "enemies of Iran" had funded the creation of 874 Iranian websites to "de-stabilize the Iranian government."[52] Jalili was referring to websites that emerged alongside opposition-led demonstrations that opposed President Mahmoud Ahmadinejad's re-election in 2009.[53]

RECRUITING IS A RUTHLESS PROCESS IN IRAN'S CYBER WORLD. TARGETED RECRUITS ARE GIVEN A CHOICE: JOIN OR JAIL.

The IRGC openly seeks hackers and utilizes criminals willing to serve state interests. Brigadier General Gholamrez Jalali stated "We welcome the presence of those hackers who are willing to work for the goals of the Islamic Republic with good will and revolutionary activities."[54] Reportedly, Iran pays bloggers and "hacktivists" seven dollars per hour to promote Iranian policies over the Internet.[55] The IRGC also plays an online role through its Center for Investigating Organized Cyber Crimes (gerdab.ir).[56] This outfit monitors Internet conversations for anti-regime comments and dialogues potentially damaging to the state.

Iranian critics would argue that Jalali's statement is no innovation. Iran has long been willing to work with any party that it feels advances its interests. Iran may use proxies to increase its cyber war capabilities and procure the tools necessary for waging cyber attacks. One proxy is Cyber Hezbollah, an online activist group that trains and motivates pro-Government Iranians in cyberspace.[57] Research presented at the International Conference on Cyber Conflict suggests that Iran has been leveraging online tools, some through the use of the IRGC, the Basij, and Ashiyane.[58]

The Basij militia, a semi-official paramilitary organization controlled by the IRGC that skeptics would argue qualifies as a criminal organization for its thuggish behavior against dissenters.[59] Established in 1979 by Ayatollah Ruhollah Khomeini, the Basij militia's mission is to defeat "Westoxification," a term Iranians use to describe the pervasive influence of Western influence on Persian culture.[60] Quoting Basij military deputy chief Ali Fazli, the official IRNA news agency bragged about how Iran has unleashed a new cyber army, which includes Basij members: "Just as we were under attack from our enemies on the web, e-trained Iranian military

experts, including Basiji teachers, students, and clerics, are attacking enemy websites."[61]

In his Congressional testimony, Homeland Security Policy Institute Director Frank J. Cilluffo stated that the Basij "provide much of the manpower for Iran's cyber-operations." Still, command and control of operations is murky. Quoting Cilluffo: "Cyberspace is a domain made for plausible deniability."[62]

Although Iran is technically proficient, it has imported many of its cyber capabilities. Ironically, Western companies have provided many of the tools used for repression. Nokia Siemens Networks, a joint venture of Finnish cellphone maker Nokia and German company Siemens, is one example as it provided the Iranian government with monitoring technology.[63] While Iran is reducing its reliance on Western technology, it has used SmartFilter, a product of the U.S.-based Secure Computing, for filtering internet content.[64] Still, one can reasonably presume that Iran will seek cyber tools from any source from whom it may be obtained, including allies like Syria, which has acquired filtering technology from the West.[65]

Iran has also acquired cyber monitoring technology from non-Western nations. Iran obtained the Israeli technology NetEnforcer after it was sold to a Danish distributor, who then resold it to Iran.[66] Blue Coat Systems Inc. manufacturers web security and filtering products that are now used in Syria. Although Bluecoat denies knowledge of how that occurred,[67] Syria's close relationship with Iran raises questions as to whether the technology was transferred to Iran. Israeli firm Allot Communications Ltd. transferred gear to RanTek A/S in Denmark that provides for "deep-packet inspection" of networks that allow email monitoring; the Danes promptly repackaged the gear and shipped it, legally under Danish law, to Iran.[68]

Stung by the bad publicity, the Italian company Area SpA cancelled construction of an internet surveillance system in Syria only after Italian newspapers picked up a Bloomberg story, sparking protests by Syrian and internet-freedom activists outside the company's headquarters and Access gathered 10,000 signatures on an online petition.[69] The project included California-based NetApp's storage hardware and software for archiving emails; probes to scan Syria's communications network from Paris-based Qosmosa SA; and gear from Germany's Ultimaco Software AG (USA) that connects tapped telecom lines to Area SpA's monitoring-center computers. Although Area SpA cancelled the contract, the remaining funds were used to pay the Iranian government to finish the installation.[70] Due to Iranian involvement with the installation, Syria's internet surveillance technology has probably wound up in Iranian hands.

In 2011, the U.S. Government Accountability Office examined whether U.S. firms were providing technology to Iran.[71] No firms were identified, although the report acknowledged that "the same technologies that enable Internet access, satellite radio and television, and cellular communications are also used or manipulated by oppressive regimes for monitoring, filtering and disrupting information and communications flows."[72]

Rather than relying solely on outside technology, Iran has developed its own

solutions for controlling cyber communications. Iran jams satellite broadcasts without special equipment by sending signals from ground sites to the satellite using the same frequency as the service disrupted and by sending jamming signals from ground or mobile-based transmitters into dishes located in cities like Tehran.[73] Iran is also developing its own filtering technology. Freedom House reports:

> *Iran now employs a centralized filtering system that can effectively block a website within a few hours across the entire network in Iran. Private internet service providers were forced to either use the bandwidth provided by the government or route [requests to visit sites] through government-issued filtering boxes developed by software companies inside Iran.*[74]

Filtering poses major challenges for the regime as Internet usage in Iran grows. Open Net Initiative (ONI) reports that in 2008 Iran had 23 million internet users (35 percent of the population) compared to one million in 2005.[75] In 2012, Khamenei issued a fatwa confirming that anti-filtering tools and software are illegal in Iran. Ironically, his use of the phrase "anti-filtering" apparently triggered Iran's filtering system, blocking Khamenei's words to most Iranians.[76]

Iran may be leveraging its relationships with China and Russia to gain a foothold in the cyber defensive and offensive world of capabilities.[77] Clearly, both allies have significant cyber capabilities which could be shared with Iran to enable it to leap-frog ahead. Amid sanctions against Iran, countries like China have filled the void in commerce, development, and relations. China, now Iran's biggest trading partner, is enjoying the continuous flow of Iranian oil.[78] Iran benefits from Chinese investment into Iranian infrastructure, valued at $1 billion. While this partnership may be originally rooted in China's energy needs and Iran's ability to fulfill those needs with oil, the relationship has developed beyond energy into something more strategic. China has deepened its partnership with Iran militarily and aided Iran considerably in its efforts to stymie the economic effects of international sanctions over its nuclear weapons program.[79]

Iran's relationship with Russia may be even more profitable in terms of technology sharing than its relationship with China. Russia continues to make pro-Iran arguments designed to deny the international community full reign over sanctions against Iran.[80] In August 2012, Russia's Foreign Ministry criticized new U.S. sanctions against Iran, labeling U.S. efforts as "undisguised blackmail."[81] Issues with Iran have strained the relationship between Russia and the U.S.; tensions have been recently exacerbated due to the delayed delivery of an advanced S-300 missile system that could hugely strengthen Iranian air defenses and complicate planning for any potential strike against Iran's nuclear program.[82] If it wants the S-300, Iran must curtail its anti-Moscow rhetoric.[83]

Leaving the Grid

Iran is trying to reduce its vulnerability to cyber attacks by changing its electronic footprint. In August 2012, Iran announced its decision to move key elements of its

ministries and state bodies off the Internet. According to Iranian Telecommunications Minister Reza Taghipour, starting in September 2012, Iran will cease sharing information about its critical infrastructure.[84] This decision is in direct response to the havoc wreaked by Stuxnet and Flame.[85] The Iranians intend to launch a domestic intranet built with a closed loop; such a system would deny Iranians access to the World Wide Web.[86]

The perception among Iranian security researchers is that Iran is among the most backward countries in terms of cyber security.[87] However, advanced countries have more to lose than less developed countries; Iran is less vulnerable to attack and exploitation. Still, as the Stuxnet attacks demonstrate, cyber tools may have a significant impact in weakening Iranian military capabilities. Current technology indicates the impact was short-term. Future malware may inflict a longer-term consequence. Its potential cyber vulnerabilities will further decline as Iran pulls its trusted entities offline and embraces greater cyber security. However, cyber experts recognize that all critical cyber infrastructure operates in an insecure environment. No one seriously believes risk can be eliminated but should be managed.

The Strategic Implications For Conflict

Cyber levels the playing field. It can protect anonymity, a critical consideration as the Law of Armed Conflict requires that responses to attack adequately identify the attackers. It enables individuals, groups, or nations like Iran to take action that creates, as Frank Cillufo has observed, a disproportionate impact:

> *This asymmetry can be leveraged by nation-states that seek to do us harm, by co-opting or simply buying/renting the services and skills of criminals/hackers to help design and execute cyber attacks against the United States...In short, no comfort can be taken from the fact that Iran lacks the sophistication of nations such as China, Russia, or the United States. Proxies for cyber capabilities are available. There exists an arms bazaar of cyber weapons. Adversaries do not need capabilities, just intent and cash.*[88]

Iran has already demonstrated it will use cyber for espionage and for wreaking havoc upon websites. It has hacked Twitter, Baidu, and Voice of America. While the hacks failed to penetrate the networks, they compromised an outside system that contained domain name service identification, acquired control of the server, and redirected traffic.[89]

Cyber attacks barrage the U.S. nuclear industry. Thomas D'Agostino of the National Nuclear Security Administration told Congress his agency faces up to 10 million events daily from a "full spectrum" of hackers, state and non-state, about 1,000 of which might be successful. Adam Segal of CFR stated that most of the 10 million daily attacks are automated bots that "are constantly scanning the Internet looking for vulnerabilities."[90] The United States' nuclear systems are "air gapped"—disconnected from standard internet systems—making it unlikely that hackers could

remotely launch a nuclear warhead. However, while unlikely, hackers could penetrate this defense; Stuxnet actually jumped an air gap to attack the nuclear centrifuges at Natanz.[91]

While serving as the Director of National Intelligence, Admiral James Clapper warned Congress that "Iran is now more willing to conduct an attack in the U.S."[92] Cillufo cited "reports that Iranian and Venezuelan diplomats in Mexico were involved in planned cyber attacks against U.S. targets, including nuclear power plants. The hackers said they were seeking passwords to protected systems and sought support and funding from the diplomats."[93]

As U.S. political leaders openly discuss the possibility of launching or supporting a strike against Iranian nuclear facilities, Iran's cyber capabilities must figure into U.S. strategy. What happens if a strike prompts Iran to launch a cyber attack that takes out power grids, aviation control towers, hospitals, or other critical infrastructure? While Iran has ostensibly made no response to the cyber attacks engendered by Stuxnet, Flame, Duqu, or Madi, these events hardly transpired in the context of a contest framed by time limits or rules of the game. Iran's leaders may elect to take action at any time and against multiple targets to prevent, counter, or even the cyber score.

Israel devotes considerable effort to pressuring Iran into abandoning its nuclear program, even resorting to a targeted anti-nuclear program cyber attack. Should Israel expect Iran to launch a cyber attack of its own? Although no cyber attack has so far inflicted irreparable damage on physical infra-structure or caused the loss of life, what is to prevent their escalation? If the Mullahs are determined to destroy Israel, cyber attacks offer an imaginative course of action to inflict extraordinary damage that, at a minimum, could irreparably ruin Israel's economy. Iran could potentially launch a cyber attack using non-state proxies impeding international assignation of blame. Israel and the international community may elect to simply fault Iran for such action. However, responding to such an attack would be complicated due to a lack of certainty and the accepted standard that response requires proportionality. The nature of any response to a cyber engagement may be complicated should Iranian allies like Russia or China choose to insist upon restraint on pain of their own intervention.

Disruption, destruction, confusion, deception, and distrust: these characteristics rank among the effects that targeted cyber strategies can achieve. The potential for Iranian mischief is great. However, Iran is not likely to engage overtly in full-fledged cyber war. Although the term has come into vogue, it is misused. The notion of an "act of war" has lent itself to statutory definitions. Pretermitting Iranian obsession with Israel, the escalatory implications render state-to-state war somewhat unlikely. As noted above, the meaning of "use of force" remains debated. Iran will not be deterred from cyber engagements, another ambivalent term that enables nation-wide flexibility in the employment of cyber tools.

Iranian influence in Bahrain, Yemen, Saudi Arabia, Lebanon, Iraq, Syria and elsewhere worries Sunni-led states and complicates the security interests of the U.S.,

which seeks to contain Iranian ambitions to expand its influence in the region. While Sunni-dominated governments may be skeptical about Iran, the threat that Iran could covertly employ cyber tools to disrupt economic institutions or to arouse political dissent could potentially have a chilling effect on their willingness to cooperate with the United States.

Sectarian competition, however, remains a factor in the strategic calculations that the U.S. and nations in the Middle East region must make in countering Iranian influence. The Shia sect comprises about fifteen percent of the 1.5 billion Muslims globally,[94] but in the broader region that stretches from Lebanon to Pakistan, the Shia and Sunni populations are about equal. Shiites account for seventy percent of those in the Persian Gulf region, representing a majority in Iran, Bahrain, and possibly Iraq,[95] the largest minority in Lebanon, and important minorities in many other nations there. Iranians see in these populations the opportunity to promote religious and political hegemony; Iran seeks to command regional respect.

Cyber tools offer targeted forms of communication to identify, persuade, and mobilize Shias to serve Iranian objectives. They offer opportunities to arouse hostility against the U.S. and other non-Muslim states. Cyber offers unique possibilities to employ confusion, misinformation, and other forms of disruption to affect the psychological mood of a country's politics and to alter, as Henry Kissinger might say, that nation's calculus of political risk.

In a region fraught with diplomatic and military sensitivity for the U.S., Iran's desire to gain regional recognition as a power figure must not be minimized. Iran's cyber capability offers opportunity to increase regional doubts about alliances with the U.S. Iran can use its cyber tools to threaten other nations, to de-stabilize any country with a Shia population, to cast a shadow over the legitimacy of monarchial regimes, and to create a different psychological equilibrium. Although a detailed inventory of potential Iranian actions lies beyond the scope of this paper, understanding Iran's capabilities and how they have utilized them at home and in limited efforts abroad—perhaps as a trial run for future action—is essential for future strategic planning.

Notes

[1] "Israel is to be wiped off the map," he declared in one of much vituperation that reflects the position of many Iranian hard-liners. "Ahmadinejad: Wipe Israel off map," *Al-Jazeera.Net*, October 28, 2005, http://www.aljazeera.com/archive/2005/10/200849132648612154.html.

[2] "Israel warns of month-long war after possible strike on Iran's nuclear program," *FoxNews.com*, August 15, 2012, http://www.foxnews.com/world/2012/08/15/israel-warns-monthlong-war-after-possible-strike-on-iran-nuclear-program/.

[3] See, e.g.: U.S. Department of Defense, Cyberspace Policy Report – A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, at 7, 9 (Nov. 2011).

[4] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *International Institute of Strategic Studies, Survival: Global Politics and Strategy* 52, no. 6, December 2010-January 2011: 127-50; and James P. Farwell and Rafal Rohozinski, "The New Reality of Cyber War," *International Institute of Strategic Studies, Survival: Global Politics and Strategy* 54, no. 4 (2012): 107-120.

[5] Robert McMillan, "Siemens: Stuxnet Worm Hit Industrial Systems," *Computerworld,* September 14, 2010, http://www.computerworld.com/s/article/9185419/Siemens_Stuxnet_worm_hit_industrial_systems.

[6] Sanger lays out his report in his book, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American*

Power, (New York: Crown, 2012): Ch. 8.
[7] *Ibid*, Ch. 8.; and "Israel Admits to Waging Cyber War on Iran," *Fars News Agency*, May 29, 2012, http://english.farsnews.com/newstext.php?nn=9103080103 (accessed May 19, 2012).
[8] See: David Albright, Paul Brannan, and Christina Walrond, "Did Stuxnet Take Out 1000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment," *Institute for Science and International Security*, December 22, 2010, http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/ ; and Michael A. Davis, "Stuxnet Reality Check: Are You Prepared for a Similar Attack?" *Information Week Analytics*, May 2011, 9.
[9] "Iran says cyber foes caused centrifuge problems," *Reuters*, November 29, 2010, http://af.reuters.com/article/energyOilNews/idAFLDE6AS1L120101129.
[10] These issues are analyzed in depth in James P. Farwell and Rafal Rohozinski, "The New Reality of Cyber War.," *International Institute of Strategic Studies, Survival: Global Politics and Strategy* 54, no. 4, 2012: 107-120.
[11] See, e.g., Dan Emory, "Making Sense of Middle East-targeted malware," *SC Magazine*, October 31, 2012: http://www.scmagazine.com/making-sense-of-middle-east-targeted-malware/article/266180/
[12] "Middle East oil firms hit by massive attacks," *Network Security*, September 2012: 2-19: http://www.sciencedirect.com/science/article/pii/S1353485812700788.
[13] "U.S. blames Iran for Renewed Attacks on American Banks," *Eurasia Review*, October 18, 2012: http://www.eurasiareview.com/18102012-us-blames-iran-for-renewed-attacks-on-american-banks/; John Leyden, "New 'Madi' cyber espionage campaign targets Iran AND Israel," *The Register*, July 17, 2012: http://www.theregister.co.uk/2012/07/17/madi_cyber_espionage_campaign/.
[14] Ellen Nakashima et al,Greg Miller and Julie Tate, "U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say," *Washington Post*, June 19, 2012, http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html.
[15] "Cyber Espionage Attacks Hit Middle East," *Journal of Turkish Weekly*, August 13, 2012, http://www.turkishweekly.net/news/140278/cyber-espionage-attacks-hit-middle-east.html
[16] Ibid.
[17] Yaakov Katz, "Iran embarks on a $1b. cyber-warfare program," *Jerusalem Post*, December 18, 2011, http://www.jpost.com/Defense/Article.aspx?id=249864.
[18] David Worthington, "Is the smart grid vulnerable to cyber warfare?" *Smart Planet*, July 25, 2012.
[19] Alex Lukich, "The Iranian Cyber Army," *CSIS*, August 13, 2012, http://csis.org/blog/iranian-cyber-army
[20] Yaakov, "Iran embarks on a $1b cyber-warfare program."
[21] Alex Lukich, "The Iranian Cyber Army.," *CSIS*, August 13, 2012.
[22] Golnaz Esfandiari, "Iran Says It Welcomes Hackers Who Work for Islamic Republic," *Radio Free Europe*, March 07, 2011, http://www.rferl.org/content/iran_says_it_welcomes_hackers_who_work_for_islamic_republic/2330495.html.
[23] "Google admits Iranian superiority in cyber warfare," *Payvand*, http://www.payvand.com/news/11/dec/1189.html.
[24] Ibid.
[25] Editorial, "Iran's Twitter Revolution," *Washington Times*, June 16, 2009, http://www.washingtontimes.com/news/2009/jun/16/irans-twitter-revolution/.
[26] Angela Moscaritolo, "Iran election protestors use Twitter to recruit hackers," *SC Magazine*, June 15, 2009.
[27] Ibid.
[28] Peter Horricks, "Stop the blocking now," *BBC News World Service*, June 24, 2009, http://www.bbc.co.uk/blogs/theeditors/2009/06/stop_the_blocking_now.html.
[29] Reza Sayah and Samson Desta, "Iran bans international journalists from covering rallies," *CNN.com*, June 16, 2009, http://www.cnn.com/2009/WORLD/meast/06/16/iran.journalists.banned/index.html.
[30] "Iran closes Al Arabiya's offices in Tehran," *Al Arabiya News*, June 14, 2009, http://www.alarabiya.net/articles/2009/06/14/75922.html.
[31] Hiawatha Bay, "Finding a way around Iranian censorship," *Boston.com*, June 19, 2009
[32] Saeed Kamali Dehghan, "Iran Protest see reinvigorated activists take to the streets in thousands," *The Guardian*, February 14, 2011, http://www.guardian.co.uk/world/2011/feb/14/iran-protests-reinvigorated-activists.
[33] Ibid.
[34] Nitasha Tiku, "Iran Tries Internet Censorship, Execution As Protesters Demand Democracy," *New York Magazine*, February 15, 2011, http://nymag.com/daily/intel/2011/02/iran_tries_internet_censorship.html; Elizabeth Flock, "Iran get back e-mail access, but other sites remain blacked out ahead of protest," *Washington Post*, February 13, 2012, http://www.washingtonpost.com/blogs/blogpost/post/iran-gets-back-e-mail-access-but-other-sites-remain-blacked-out-ahead-of-protests/2012/02/13/glQAgxz5AR_blog.html.

[35] "Special Internet Court To Be Set Up Into be set up in Iran Following Launch Of Internet Filtering Project," *Middle East Media Research Institute* (MEMRI), citing *Rooz*, December 3, 2008; *Fars New Service*, December 1, 2008; and *Sobh-e Sadeq*, November 3, 2008, http://www.thememriblog.org/blog_personal/en/11867.htm.
[36] Thomas Erdbrink, "Iran Cyber police cite U.S. threat," *Washington Post*, October 29, 2011, http://www.washingtonpost.com/world/middle_east/iran-cyber-police-cite-us-threat/2011/10/27/gIQA1yruSM_story.html.
[37] Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom*, (New York: Public Affairs, 2011).
[38] Evgeny Morozov, "Iran: Downside to the 'Twitter Revolution," *Dissent*, Fall 2009, http://www.evgenymorozov.com/morozov_twitter_dissent.pdf.
[39] Ibid.
[40] Evgeny, Ibid.
[41] Ibid.
[42] Golnaz Esfandiari, "Iran Says it Welcomes Hackers Who Work for Islamic Republic," *Radio Free Europe*, March 07, 2011, http://www.rferl.org/content/iran_says_it_welcomes_hackers_who_work_for_islamic_republic/2330495.html.
[43] Farvartish Rezvaniyeh, "Pulling the Strings of the Net: Iran's Cyber Army," *Frontline*, February 26, 2010, http://www.pbs.org/wgbh/pages/frontline/tehranbureau/2010/02/pulling-the-strings-of-the-net-irans-cyber-army.html.
[44] Golnaz Esfandiari, "Iran Says it Welcomes Hackers Who Work for Islamic Republic," *Radio Free Europe*, March 07, 2011.
[45] Nate Anderson "Iranian Cyber Army Attacks Voice of America website," *Ars Technica*, February 22, 2011, http://arstechnica.com/tech-policy/2011/02/iranian-cyber-army-attacks-voice-of-america-website/.
[46] Jim Finkle and Diane Bartz, "Twitter hacked, attacker claims Iran link," *Reuters*, December 18, 2009, http://www.reuters.com/article/2009/12/18/us-twitter-idUSTRE5BH2A620091218.
[47] Ibid.
[48] Jeremy Kirk, "Iranian Cyber Army running botnets, researchers say," *Computerworld*, October 25, 2010, http://www.computerworld.com/s/article/9192800/Iranian_Cyber_Army_running_botnets_researchers_say.
[49] Amy Kellog, "Iran is Recruiting Hacker Warriors for its Cyber Army to Fight 'Enemies'," *Fox News*, March 14, 2011, http://www.foxnews.com/world/2011/03/14/iran-recruiting-hacker-warriors-cyber-army/.
[50] Statement of Frank J. Cilluffo, Director, Homeland Security Policy Institute, The George Washington University, before the Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence and Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, Washington, DC, April 26, 2012April 26, 2012, 5, citing Iftach Ian Amit, "Cyber[Crime|War]," paper presented at DEFCON 18 conference, July 31, 2010.
[51] Farvartish Rezvaniyeh,, "Pulling the Strings of the Net: Iran's Cyber Army,," *Frontline*, February 26, 2010, http://www.pbs.org/wgbh/pages/frontline/tehranbureau/2010/02/pulling-the-strings-of-the-net-irans-cyber-army.html; and Robert F. Worth, "Iran: Opposition Web Site Disrupted," *The New York Times*, December 18, 2009, http://query.nytimes.com/gst/fullpage.html?res=9907E0DF1530F93AA25751C1A96F9C8B63.
[52] "Iran unleashes 'cyber army,'" *ABS-CBN News*, March 14, 2011, http://www.abs-cbnnews.com/global-filipino/world/03/14/11/iran-unleashes-cyber-army.
[53] "Iran cyber army 'target enemy sites,'" *AFP*, May 14, 2011: http://www.google.com/hostednews/afp/article/ALeqM5h3IbvB9Ztn-J-bOdLZtwNz3DdtSA?docId=CNG.5f260e64e119410610fba84308cdfd97.841.
[54] Golnaz Esfandiari, "Iran Says it Welcomes Hackers Who Work for Islamic Republic.," *Radio Free Europe*, March 07, 2011.
[55] David Inserra, "Iran Is Serious About Cyber," *The Foundry*, June 8, 2012, http://blog.heritage.org/2012/06/08/iran-is-serious-about-cyber/.
[56] Ibid.
[57] Frank Cilluffo, "Preparing for a More Aggressive Iran," *Huffington Post*, 30 July 30, 2012, http://www.huffingtonpost.com/frank-j-cilluffo/preparing-for-a-more-aggr_b_1718725.html.
[58] Cyrus Farivar, "Iranian Gov't Pays Paramilitary Hackers, Bloggers to Bring You Islamic Revolution 2.0," *ARS Technica*, June 6, 2012, http://arstechnica.com/tech-policy/2012/06/iran-expands-online/.
[59] See: Jon Lee Anderson, "Understanding the Basij," *New Yorker*, June 19, 2009.
60 David, "Iran Is Serious," *The Foundry*, June 8, 2012.
[61] "Iran unleashes 'cyber army,'" *ABS-CBN News*, March 14, 2011, http://www.abs-cbnnews.com/global-filipino/world/03/14/11/iran-unleashes-cyber-army.
[62] Statement of Frank J. Cilluffo, Director, Homeland Security Policy Institute, George Washington

University, before the Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence and Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, April 26, 2012, 5.
63 Brian Stelter and Brad Stone, "Web Pries Lid of Iranian Censorship," *The New York Times*, June 23, 2009, http://www.nytimes.com/2009/06/23/world/middleeast/23censor.html?_r=0.
64 Open Net Initiative: "Internet Filtering in Iran in 2004-2005: A country study." *OpenNet Initiative*, http://opennet.net/studies/iran.
65 See, e.g.: Ben Wagner, "Exporting Censorship and Surveillance Technology," *Humanist Institute for Co-Operation with Developing Countries* (HIVOS), January (2012): 9.
66 Ben Elgin, "Israel Didn't Know High-Tech Gear Was Sent to Iran," *Bloomberg*, December 23, 2011.http://www.bloomberg.com/news/2011-12-23/israel-didn-t-know-high-tech-gear-was-sent-to-iran-via-denmark.html.
67 Ben Wagner, "Exporting Censorship and Surveillance Technology," *Humanist Institute for Co-Operation with Developing Countries* (HIVOS), January 2012, http://www.hivos.net/Hivos-Knowledge-Programme/Themes/Digital-Natives-with-a-Cause/Publications/Exporting-Censorship-and-Surveillance-Technology: 8; and "#OpSyria: Web censorship Technologies in Syria revealed [EN]," *Reflets*, (2011), http://reflets.info/opsyria-web-censorship-technologies-in-syria-revealed-en/.
68 Ben Elgin, "Israel Didn't Know High-Tech Gear Was Sent to Iran," *Bloomberg*, December 23, 2011.
69 *Ibid*; and: Ben Elgin and Vernon Silver, "Syria Crackdown Gets Italy Firm's Aid With U.S.-Europe Spy Gear," *Bloomberg*, November 3, 2011, http://www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear.html.
70 Ben Elgin and Vernon Silver, "Syria Crackdown Gets Italy Firm's Aid with U.S.-Europe Spy Gear."
71 U.S. Government Accountability Office. Report GAO-11-706R, Washington, DC, June 30, 2011. The Comprehensive Iran Sanctions, Accountability and Divestment Act of 2010 (CISADA), 22 U.S.C. 8515 bans the export of technologies to the Iranian government for monitoring, filtering, and disrupting information and communication flows.
72 Ibid, 7.
73 Ibid, 8.
74 "Freedom on the Net 2011: A Global Assessment of Internet and Digital Media," *Freedom House*, (Washington/New York), April 18, 2011, http://www.ifap.ru/library/book497.pdf.
75 Open Net Initiative, June 16, 2009. See also: International Telecommunications Union, "ITU Internet Indicators 2008."
76 Cyrus Farivar, "Iran's Web censorship filters supreme leader's own statement," *Ars Technica*, May 9, 2012, http://arstechnica.com/tech-policy/2012/05/irans-web-censorship-filters-supreme-leaders-own-statement/.
77 See: Ilan Berman, "Cyberwar and Iranian Strategy," *AFPC Defense Dossier*, August 2012.
78 "China: The Latest Invasion," *The Economist*, August 18, 2012, http://www.economist.com/node/21560614.
79 Scott Warren Harold and Alireza Nader, "China and Iran: Economic, Political, and Military Relations," Rand, http://www.rand.org/content/dam/rand/pubs/occasional_papers/.
80 Eric Walberg, Eurasia Review, "Russia in the Middle East: Return of a Superpower?" *Eurasia Review*, Aug 17, 2012, http://www.eurasiareview.com/17082012-russia-in-the-middle-east-return-of-a-superpower-oped/
81 "Russia Slams new US Sanctions on Iran," *Associated Press*, August 14, 2012 http://news.yahoo.com/russia-slams-us-sanctions-iran-184328355.html.
82 "Iran-, Russia: Lawsuit Puts Relations at Risk," *Kommersant*, August 16, 2012, http://rbth.ru/articles/2012/08/16/iran-russia_lawsuit_puts_relations_at_risk_17429.html.
83 "Russia and Iran: Heading for Divorce Court?" *Russia Today*, August 10,2012, http://rt.com/politics/russia-iran-s300-court-nuclear-weapons-349/; See also: "Friday Prayers and Anti-Russian Slogans," *Stratfor*, July 17, 2009; and: Sergey Strokan, "Russian and Iran: Heading toward a political earthquake," *RT.Com*, August 15, 2012.
84 "Iran Won't Anymore Air Critical Infrastructure Online," *SPAMfighter*, August 13, 2012, http://www.spamfighter.com/News-17879-Iran-Wont-Anymore-Air-Critical-Infrastructure-Online.htm.
85 "Iranian state to go offline over cyber attacks," *Voice of Russia*, August 6, 2012, http://english.ruvr.ru/2012_08_06/Iranian-state-to-go-offline-over-cyber-attacks/.
86 Joseph Sarkisian, "Iran Cyber Attack on Nuclear Facilities Leads Regime to Threaten Shutting Down the Internet," *Policymic*, August 17, 2012, http://www.policymic.com/articles/12970/iran-cyber-attack-on-nuclear-facilities-leads-regime-to-threaten-shutting-down-the-internet.
87 "Iran Won't Anymore Air Critical Infrastructure Online."http://www.spamfighter.com/News-17879-Iran-Wont-Anymore-Air-Critical-Infrastructure-Online.htm.
88 Statement of Frank J. Cilluffo, 4.
89 Alex Lukich, "The Iranian Cyber Army," *CSIS*, August 13, 2012, http://csis.org/blog/iranian-cyber-army.

[90] Jason Koebler, "U.S. Nukes Face up to 10 Million Cyber Attacks Daily," *US News & World Report*, March 20, 2012, http://www.usnews.com/news/articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily.
[91] Ibid.
[92] Ibid; and Testimony of James R. Clapper before the Senate Select Committee on Intelligence, Worldwide Threat Assessment of the US Intelligence Community, January 31, 2012, Washington, D.C.
[93] Statement of Frank J. Cilluffo; and S. Smithson, "U.S. authorities probing alleged cyber attack plot by Venezuela, Iran," *Washington Times*, December 13, 2011, http://www.washingtontimes.com/news/2011/dec/13/us-probing-alleged-cyberattack-plot-iran-venezuela/?page=all.
[94] Roula Khalaf, "New Order fans fears of Shia Crescent," *Financial Times*, June 18, 2008; and Jason Burke, "Are the Shias on the brink of taking over the Middle East?" *The Observer*, July 23, 2006, http://www.guardian.co.uk/world/2006/jul/23/israel.syria.
[95] Henry Kissinger, "On China," (New York: Penguin Press, 2011), 129.