AFTER THE GREEN MOVEMENT:

INTERNET CONTROLS IN IRAN, 2009-2012

OPENNET INITIATIVE | FEBRUARY, 2013

www.opennet.net/iranreport2013

FOREWORD

After the Green Movement is a report produced by the Citizen Lab as part of our contribution to the OpenNet Initiative (ONI). The OpenNet Initiative is a collaborative partnership of three institutions: the Citizen Lab at the Munk School of Global Affairs, University of Toronto; the Berkman Center for Internet & Society at Harvard University; and the SecDev Group (Ottawa).

This report was co-authored by the following ASL19 and Citizen Lab researchers: Matthew Carrieri, Ali Karimzadeh Bangi, Saad Omar Khan, and Saffron Suud. Ron Deibert provided guidance and editorial oversight. Masashi Crete-Nishihata, Jakub Dalek, and Adam Senft provided research assistance. Jacqueline Larson provided editorial assistance. Jane Gowan produced the layout design. We are grateful to Helmi Noman for research inputs.

TABLE OF CONTENTS

KEY FINDINGS

- Since the “Green Movement” protests in 2009, the Iranian regime has adopted increasingly complex surveillance and monitoring techniques, complementing technical filtration tools with legal frameworks and information manipulation.

- These techniques of control overlap: technical filtering is reinforced by a more constricted legal environment and efforts to “nationalize” Iranian cyberspace.

- ONI testing over the past several years has revealed consistent filtering of websites pertaining to social media, international news channels, non-Shi’ite religions, social and religious taboos, and anything remotely opposed to official government policies.

- The creation of a “Supreme Council on Cyberspace” indicates the Iranian government’s interest in centralizing their approach towards the Internet as well as their view of cyberspace as a larger security concern.

- Internet censorship in Iran—culminating in the National Information Network—is framed as a way to protect the nation’s unique culture and identity and defend against the onslaught of Westernization.

- The Iranian regime considers cyberspace a geopolitical as much as a domestic policy realm. Surveillance and censorship are simultaneously tools of suppression and a means of national defence.

INTRODUCTION

In 2009, protests erupted across Iran in opposition to the victory of the incumbent conservative president, Mahmoud Ahmadinejad, over his reformist challenger, Mir-Hossein Mousavi, in the presidential elections. Mousavi and other opposition candidates roundly denounced the election results, which were pronounced only two hours after polls closed on 12 June 2009 and claimed Ahmadinejad had captured well over 60 percent of the vote. Supporters of Mousavi took to the streets in Tehran shortly thereafter and protests gradually spread to other major cities over the following weeks. Those calling for Ahmadinejad's overthrow clothed themselves in green—Mousavi's campaign colour—thereby spawning the "Green Movement." The regime swiftly and violently attempted to put down any sign of popular unrest in the country by arresting, beating, and firing upon pro-opposition protesters. Despite such violence, mass demonstrations continued sporadically throughout 2010 and 2011.

Western media heralded the Green Movement in Iran as a "Twitter revolution" fueled by information and communication technologies (ICTs) and social media tools.[1] Activists and bloggers both inside and outside of the country used Twitter, Facebook, and YouTube to broadcast a constant stream of news updates, photos, and video clips depicting the violence perpetrated by the regime and its security apparatus. As Mehdi Yahyanejad and Elham Gheytanchi note, "citizen journalism via social media made it possible for news to flow from Iran despite government censorship of the Internet and bans on foreign-media coverage."[2] Meanwhile, hacktivists and software engineers based in Iran and abroad kept Internet channels open through proxy portals and virtual private networks (VPNs), as the government scrambled to block them. ICTs thus played a pivotal role in helping Iranian social movements circumvent media blackouts to organize themselves and exchange information with the rest of the world.

If the post-election protests were indeed indicative of a supposed "Twitter revolution," then one would expect the Iranian regime to respond by cracking down on ICTs and social media. After all, ever since Iran connected to the global network in 1993, authorities have maintained a volatile relationship with the Internet —becoming increasingly aggressive as the Internet's social, political, and economic significance has grown inside the country. The government's stance toward the Internet, however, has been conflicted: ICTs are viewed by the authorities as both a means toward

[1] "Iran's Twitter revolution." *The Washington Times*, 16 June 2009. http://www.washingtontimes.com/news/2009/jun/16/irans-twitter-revolution/ (accessed 24 October 2012).

[2] Mehdi Yahyanedjad and Elham Ghetytanchi, "Social Media, Dissent, and Iran's Green Movement" in *Liberation Technology: Social Media and the Struggle for Digital Diplomacy*, ed. Larry Diamond and Marc F. Plattner (Baltimore: Johns Hopkins University Press, 2012), 140.

sustained economic and political strength, and as tools of espionage in the hands of the opposition. This report examines whether the tools, techniques, and practices of censorship and surveillance in Iran have discernibly changed since 2009. After 2009, the Iranian government took a number of steps toward tightening its grip on digital information flows. In essence, the Iranian regime's turn toward overarching legal frameworks and information manipulation to complement filtration tools, which proved incapable of preventing the "Green Movement," has accelerated since 2009. The Green Movement's use of ICTs to organize demonstrations and communicate with the outside world exposed simple filtering mechanisms' inability to stifle dissent. Instead, the government pursued comprehensive legal and regulatory changes aimed at centralizing control of the Internet and privately owned Internet service providers (ISPs) in the hands of the newly formed Supreme Council on Cyberspace, while simultaneously criminalizing access to banned websites. At the same time, the state has fought to promote its own national narrative in cyberspace by developing a "National Internet" and by at least tacitly encouraging the aggressive dissemination of its ideology through groups like the "Iran Cyber Army."

Iran is not simply a cookie-cutter example of an authoritarian regime moving toward more sophisticated Internet controls. Two factors distinguish Iran as a unique case that merits its own study. The first is Iran's invocation of a very particular rhetoric to legitimize the filtering of websites and monitoring of netizens. The Iranian regime strives to present its actions as defensive manoeuvres against the onslaught of "Westernization" and thereby aims to protect what it sees as an increasingly endangered culture. The second unique characteristic is the extent to which geopolitical factors play a key role in the Iranian government's cyberspace policies. Iran has expressed particular concern over the West's exercise of power in cyberspace, including "soft" tactics like propaganda and "hard" tactics like targeted malware attacks. Such attacks have been especially visible since 2010 because Iran has accused the United States and Israel of unleashing a series of targeted malware attacks against its nuclear facilities.[3] These accusations have now been supported by purported leaks from the Obama administration and reported in the *New York Times*.[4] Thus, Internet censorship, surveillance, and other information controls—both technical and legal—are not merely tools for suppressing domestic dissent. They are also offensive and defensive weapons in an increasingly militarized cyberspace.

[3] Gregg Keizer, "Iranian General Accuses Siemens of Helping U.S., Israel Build Stuxnet," *Computer World*, 18 April 2011, https://www.computerworld.com/s/article/9215901/Iranian_general_accuses_Siemens_of_helping_U.S._Israel_build_Stuxnet (accessed 21 October 2012).

[4] David E., Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, 1 June 2012, https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all (accessed 24 October 2012).

THEORY: GENERATIONS OF CONTROLS

The nature of Iran's censorship regime has changed over the years, with censorship in its various manifestations growing and becoming more entrenched in Iranian society and politics. In their discussion of content controls in Russian cyberspace, Deibert and Rohozinski conceptualize censorship and information controls as multigenerational, with multiple layers of control often existing simultaneously.[5] This progression applies neatly to the evolution of Iranian information controls in cyberspace. Three generations of control constitute this model:

- First-generation controls restrict access to specific Internet resources and sites, through technical filtering and physical monitoring by state security (e.g., monitoring of Internet cafés).
- Second-generation controls create normative, legal, and regulatory environments in which content controls can be legalized, and develop technical capabilities to create "just-in-time" content controls that deny access to specific information during key moments when that information may be at its highest value.
- Third-generation controls aim to create "cognitive change" rather than deny access to information. Examples include state use of sophisticated means of online surveillance or "information" campaigns to discredit opponents.

First-generation controls are, arguably, the most basic means with which the state can deny access to prohibited information in cyberspace. These controls are also, however, not insurmountable. In Iran, for example, citizens have used proxies, VPN services, and other censorship-circumvention tools to access sites otherwise unavailable in the country due to the pervasive regime of national Internet filtering.

Second-generation controls raise the level to which a state is willing to control online expression. Some of these approaches can be nontechnical and very open, such as the passing of new, specific legislation aimed at controlling expression in cyberspace, or the citing of existing press, sedition, and other laws to stifle such expression. In the case of Iran, Internet-specific legislation has made strict controls over online activity very clear to Internet users in the country. The regime also arbitrarily enforces generalized laws, such as the Press Law, to stifle dissent at will. Other second-generation controls are more surreptitious and technical. These methods allow states to enact "just-in-time" blocking, to deny particular vectors of information at politically sensitive moments in time

[5] Ronald Deibert and Rafal Rohozinski, "Control and Subversion in Russian Cyberspace," in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, ed. Ronald Deibert, John Palfrey, Rafal Rohozinkski, and Jonathan Zittrain. (Cambridge, MA: MIT Press, 2010), 15-34.

(for example, Iran's blocking of Secure Socket Layer [SSL] traffic in February 2012).

Third-generation controls are considered more difficult to document. Highly sophisticated and multidimensional, they focus less on denying access to information and more on promoting a particular national narrative in cyberspace as part of a competition of ideas and ideologies. The creation of national cyberzones (e.g., Iran's National Information Network) is an effective means of inhibiting the open and free exchange of information that the Internet provides. Attacking the dissenting views of internal or external actors by permitting the actions of "Internet brigades" (e.g., information operations conducted by Iran's so-called Cyber Army) is another method whereby a state (or non-state actors supporting the regime with or without explicit state support) can fight its own information war and project ideas that are favourable to its national ideology. Enhancing the existing cyber-capabilities of a nation's armed forces is yet another example of a third-generation control. In light of recent malware attacks that the government interpreted as specifically directed against its nuclear facilities, Iran has made efforts to bolster its military institutions against cyberwarfare contingencies.

BACKGROUND: ICT INFRASTRUCTURE AND FILTERING

The Iranian regime has long exerted control over the Internet by filtering content and blacklisting websites. While online free speech was relatively unregulated during the 1990s, the OpenNet Initiative has documented a clear politicization of the Internet throughout the 2000s.[6] Conservative political factions cracked down on print and broadcast journalists during Mohammad Khatami's reformist government (1997-2005), pushing political writers to the Internet as the only remaining vehicle for free expression.[7] As the Internet became a platform for Iranians to publish opinions critical of the regime or to expose controversial issues, authorities sought to monopolize the telecommunications industry and control the content made available.

INDUSTRY AND INFRASTRUCTURE

The very structure of the telecommunications industry in Iran lends itself to government control. The Ministry of Information and Communications Technology (MICT) runs the Telecommunication Infrastructure Company (TIC), which has a monopoly over the purchase of international Internet gateways in Iran.[8] The TIC provides Internet bandwidth and maintains international and local traffic's capacity for both the public and private sectors.[9] The Telecommunication Company of Iran (TCI), which operates the TIC, owns the Data Communication Company of Iran (DCI), which is the main ISP in the country. The TCI was supposed to be privatized beginning in 2007 but the Iranian Revolutionary Guard Corps (IRGC) took advantage of its initial public offering in September 2009 to expand their role in Iran's telecommunications sector. One of the IRGC's companies—the Mobin Trust Consortium—purchased over 50 percent of the TCI's shares in what is considered the biggest deal in the history of Iran's stock exchange.[10] The IRGC's majority ownership of the TCI effectively renders it a state-owned enterprise and further consolidates the government's total control over telecommunications.

[6] *Internet Filtering in Iran in 2004-2005: A Country Study*, Open Net Initiative, http://opennet.net/studies/iran#app1 and *Internet Filtering in Iran 2006-2007*, Open Net Initiative, http://opennet.net/studies/iran2007 and *Iran*, Open Net Initiative, http://opennet.net/research/profiles/iran.

[7] "Iran: Journalists Under Siege," *Amnesty International*, 30 April 2010, http://www.amnesty.org/en/news-and-updates/iran-journalists-under-siege-2010-04-30 (accessed 25 October 2012).

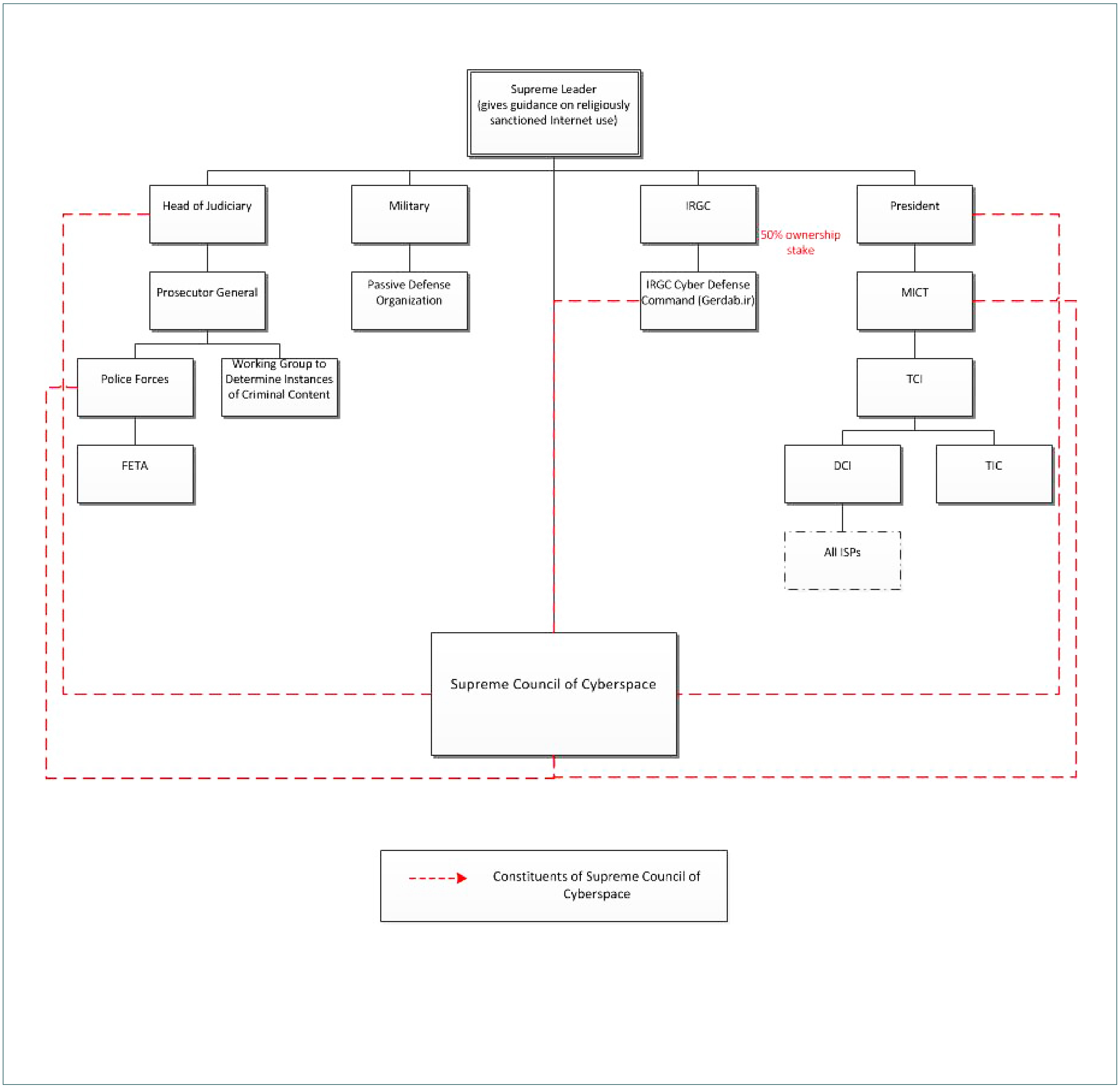
[8] "Telecommunication Infrastructure Company of Iran after eight years," *ICTNA News Agency*, http://www.ictna.ir/id/043699/ (accessed 23 November 2012)

[9] "Telecommunication Infrastructure Company," *Ministry of ICT*, http://www.ict.gov.ir/introduction-affileted-tic-en.html (accessed 29 April 2010).

[10] "Explanation to Parliament About IRGC's Purchase of TCI Shares," [in Farsi] *BBC Persian*, 25 May 2010, http://www.bbc.co.uk/persian/iran/2010/05/100525_l38_irantelecom_stockexchange_kavakebian_hoseini.shtml (accessed 18 August 2010).

Ultimately, all public Internet traffic is routed through the TCI. Privately owned ISPs must connect through the company to offer Internet access to the public. It is also the only ISP authorized to supply government agencies. This single point of connection makes it easy for the government to control the Internet and effectively filter it either by blocking webpages or blacklisting keywords. The TCI uses proxy servers that facilitate government surveillance by logging all unencrypted Internet traffic, including e-mails, browsing information, and instant messages.

FIGURE 1: HIERARCHY OF INTERNET INSTITUTIONAL STRUCTURE


Supreme Leader (gives guidance on religiously sanctioned Internet use)
Head of Judiciary
Military
IRGC
President
50% ownership stake
Prosecutor General
Passive Defense Organization
IRGC Cyber Defense Command (Gerdab.ir)
MICT
Police Forces
Working Group to Determine Instances of Criminal Content
TCI
FETA
DCI
TIC
All ISPs
Supreme Council of Cyberspace
Constituents of Supreme Council of Cyberspace

One other body directly connected to the global network is the government-sponsored Institute for Research in Fundamental Sciences, which serves as the domain name registry of ".ir" domain names.[11] All private ISPs, which include Pars Online, Shatel, Datak Telecom, AfraNet, Soroush Rasaneh, and Pishgaman-e Kavir among others, are therefore indirectly licensed by the government. Even the ISPs that maintain their own satellite Internet infrastructure—for example, Pars Online—are licensed by the state.[12]

The Telecommunications Infrastructure Company (TIC) provides international connections "by fiber optic links through Jask-Fojeyreh and Falkon in the South of Iran, and maintains a backup transit in the North-West from Tabriz to Ankara and Istanbul in Turkey."[13] In late February 2010, TIC signed a contract with Iran Mobin Company to install a fiber optic link, similar to Falkon in the country's south, through the Caspian Sea to Azerbaijan and Russia.[14] Iran Mobin from Iran, AZTelekom from Azerbaijan, and Synetra from Russia would work together to expand Iran's Internet infrastructure in the North, linking it to Europe via Russia. In 2010, Rostelecom of Russia also stepped in as a major transit provider to the DCI. Rostelecom has been described as the third-most important provider for Iran's international transit, behind Turk Telekom (Turkey) and TeliaSonera (Sweden).[15]

FILTERING PRACTICES

Iran's filtering system is among the most extensive in the world, but technical details about it remain limited. A series of decrees issued by the Supreme Council of the Cultural Revolution (SCRC) in December 2001 formed the institutional basis for Iran's filtering practices. Until recently, ISPs were required to filter websites based on criteria set by the Committee in Charge of Determining Unauthorized Sites (CCDUS).[16] However, with the adoption of the Cyber Crimes Law (discussed below) the CCDUS was replaced by the Working Group to Determine Instances of Criminal Content within the Ministry of Justice.[17] The actual implementation of filtering is the responsibility of the Information Technology Company of Iran (ITC), a TCI subsidiary. Below are some of the activities that activists have found in Iran related to the government's filtering methods:

- Shallow inspection at ISP level: HTTP is inspected to check if domain names match blacklisted websites. Shallow inspection also monitors URLs for blacklisted keywords.
- Firewall-and traffic-shaping boxes: These methods have been used to filter key ports. Yahoo Messenger and HTTPS ports have

[11] "About IPM," *Institute for Research in Fundamental Sciences,"* http://www.ipm.ac.ir/about-IPM.jsp

[12] Craig Labovitz, "Behind the Firewall – A Look at Six Iranian ISPs Forty Days," *The Arbor Networks Security Blog*, 3 August 2009, http://asert.arbornetworks.com/2009/08/1132/ (accessed 18 September 2010).

[13] "Iran Mobin Installs Fibre Optic Ring," [in Farsi] *Asr-e Ertebatat Weekly*, 27 February 2010, http://asreertebat.com/1388/12/8/AsreErtebat_weekly/348/Page/8/ (accessed 29 April 2010).

[14] Ibid.

[15] James Cowie, "The Geopolitics of Iranian Connectivity," *Renesys Blog*, 11 February 2010, http://www.renesys.com/blog/2010/02/irans-internet-the-geopolitics.shtml.

[16] "Iran," in *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace*, ed. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2010), 548.

[17] "Introduction", The Working Group to Determine Instances on Online Criminal Content, http://internet.ir/intro.html (accessed 23 November 2003)

been blocked at different points in time via this technology.

- IP-based filtering: Websites such as Facebook have been blocked through IP-based filtering. For example, all packets containing Facebook.com IP addresses in their destination were dropped.
- Random packet dropping: This method is perhaps one of the most successful filtering techniques used in Iran. It effectively slows down the Internet and stops users from uploading content. Periodically, all VPN technologies (including GRE, PPTP, L2TP, IPSec) as well as encryption protocols like SSH and IP-in-IP layer 3 are filtered.

In 2011, ONI conducted a series of tests on nine ISPs in Iran, using a total sample of approximately 2,000 URLs. June 2011, marked the second anniversary of the contested 2009 presidential election when the country launched a major online offensive by blocking websites and arresting online activists. Over the course of the month, ONI tested approximately 1700 URLs on Samaneh Sama Pishro ISP, of which 616 were blocked. ONI used the same list to test on four other ISPs in June: DCI Autonomous System on June 17-18, Mobin Net on June 21, Metanet Sepahan Technology Co. on June 23-24, and Farhang Azma Communications Company LTD on June 23-26. All produced similar results. A second round consisting of approximately 1,580 URLs occurred in mid to late November 2011, with multiple test runs on the University of Tehran ISP and a single test run on Rasana. The testing list changed significantly between June and November 2011, when 30 local URLs were added and roughly 150 dead global links removed. As such, cross-temporal comparisons are necessarily limited. The November tests found that all URLs blocked on Rasana were also blocked on the University of Tehran, though the reverse is not true. These results seem to suggest that universities and similar institutions with relatively high proportions of intellectual or youth in their user bases are subject to heavier filtering. As expected, political opposition and pornography websites, in addition to websites with freedom-of-expression-related content, were found to be systematically blocked across ISPs. A third round of testing occurred in September 2012, using a list largely identical to that of November 2011, on two ISPs: Pars and Shatel. No significant change in filtering practices on those websites was discernible. ONI added websites specifically related to, or detailing information about, rebel forces and opposition to the Syrian regime, as well as non-Shi'ite religious pages. Those results are detailed in Box 1. (For a full list of URLs blocked, see: https://citizenlab.org/data/iranreport/.)

BOX 1: ONI TESTING ANALYSIS

- "Internet Filtering in Iran in 2004-2005" made the point that Farsi sites were more consistently blocked than English sites at the time.[1] English-language news sites in particular were not as heavily blocked as Farsi ones. In 2009, more English language news sites were blocked (bbc.co.uk being a notable one, blocked after the June election protests, with the BBC Persian language service blocked in January 2006). The trend continued in the 2011 tests, with bbc.co.uk and bbc.co.uk/persian still blocked across ISPs, along with other international news sites such as cbc.ca, cbsnews.com, foxnews.com, and guardian.co.uk, among others.

- Facebook and Twitter continue to be blocked. ONI previously reported that Facebook was blocked—amid considerable domestic controversy—in May 2009, possibly as a means for the ruling government to prevent online political organization by supporters of reformist candidate Mir-Hossein Mousavi prior to the elections.

- Blog-hosting services wordpress.com, blogspot.com, and blogger.com were found to be blocked on all ISPs tested in 2011. In 2009, ONI reported that the focus was on blocking individual blogs, although hosting services like livejournal.com and xanga.com were blocked. (They remain blocked in 2011).

- YouTube, which was periodically available in 2009 (but was blocked after the June 2009 elections) remains blocked on all ISPs.

- Tests results show that Iran blocks several websites of regional Arabic media known to have critical reporting on Iran. Examples include the website of Al-Arabia TV (http://www.alarabiya.net) and the London-based pan-Arab newspaper *Asharq Al-Awsat* (http://www.aawsat.com). Both Al-Arabia TV and *Asharq Al-Awsat* are Saudi funded and are known to propagate the official Saudi editorial policy which is often critical of Iran. The website of the UAE-based newspaper *The National* (http://www.thenational.ae) is also blocked, likely due to reporting on Abu Musa, a disputed Persian Gulf island that is currently controlled by Iran but also claimed by the UAE. *The National* has consistently supported the official stance of the UAE and Gulf states.[2] Several Western media websites are also blocked, including BBC English and Arabic, CNN, and ABC.

- Iran blocks websites of non-Islamic religious such as the Bahai faith (http://www.bahai.org), but also content relevant to Sunni Islam, which is not the official branch of Islam in Iran (Shi'ism). Examples include the official website of the Sunni community in Iran (http://www.sunnionline.us/arabic/), websites that provide news about Sunni communities (http://sunni-news.net/), websites that explain Sunni doctrine (http://www.islamway.net/) and websites that serve as a platform for religious discussion on Sunni Islam (http://www.ansarsunna.com/vb/).

- A number of keywords were tested that could potentially yield explicit content. Many of them were found to be blocked. Using Yahoo, the following keywords were blocked and yield a block page: *porn*, *sex*, *fuck*, *gay*, and *lesbian*. We also tested a number

[1] "Internet Filtering in Iran in 2004-2005: A Country Study." OpenNet Initiative. N.p.. Web. 23 Oct 2012. http://opennet.net/studies/iran.

[2] See, for example: Mahmoud Habboush. "Iran's occupation of Gulf islands 'shameful', says Minister." The National. April 21 2010. Web. 23 Oct 2012. <http://www.thenational.ae/news/uae-news/irans-occupation-of-gulf-islands-shameful-says-minister> and Peter Hellyer. "Iranian claims to disputed islands whitewash history." The National. April 18 2012. Web. 23 Oct 2012. <http://www.thenational.ae/thenationalconversation/comment/iranian-claims-to-disputed-islands-whitewash-history>.

of Farsi terms such as the one for "homosexuality" and found them to be blocked. Keyword filtering also applies to URLs that contain objectionable words regardless of the website's content. For example, the website http://www.no-porn.com/ is blocked apparently because the word "porn" is in the URL even though the website is about providing support to porn addicts. Yahoo's image search was blocked regardless of what keyword was used — attempts to search for images using the keywords Iran and Islam yielded a block page. Likewise, attempts to turn off SafeSearch on Google Images and Google Videos also invoked the block page.

- URLs within Israel's country code top-level domain (ccTLD) are blocked in Iran. All .il URLs are blocked regardless of their content. We tested the website of Israel's Ministry of Foreign Affairs (http://www.mofa.gov.il/mfa) as well as other commercial and business websites such as http://www.accubeat.co.il/, http://www.discountbank.co.il/wps/portal/hebrew/, http://www.made.co.il/, http://www.walla.co.il/, and http://www.issta.co.il/. Apparently Iran implements a blanket policy on all .il URLs: when we tested a non-existent URL (http://www.ThisSiteDoesNotExist.il/), we received the blockpage instead of an error message.

- Iran blocks a variety of websites in various content categories. For example, the website of Columbia University is blocked, likely a result of university president Lee Bollinger's harsh criticisms of Iranian president Mahmoud Ahmadinejad in September 2007.[3] We also found that Citizen Lab's website (citizenlab.org) is blocked. Although we cannot determine the reason for certain, it is probably because of the research that the lab has conducted on Iran, which reveals in an academically neutral way the filtering and surveillance practices of the Iranian regime.

- Websites operated by or otherwise about the Syrian opposition to Bashar al-Assad's government were not blocked unless they were hosted by Blogspot, which is subject to blanket filtering. These results were somewhat unexpected, given the lengths to which the Iranian regime has gone to prevent domestic media from covering the ongoing civil conflict in Syria (see Box 4).

[3] CNN, "Columbia University president slams Ahmadinejad." Last modified September 24, 2007. Accessed October 23, 2012. http://articles.cnn.com/2007-09-24/us/columbia.president_1_iranian-leader-lee-bollinger-mahmoud-ahmadinejad?_s=PM:US.

End of Box 1

The breadth and scope of filtering in Iran expands far beyond these topics. According to a 2008 study conducted by John Kelly and Bruce Etling, Iran's blogosphere is one of the most diverse and vibrant in the world, with some 60,000 active blogs in Farsi.[18] However, it is also heavily filtered — ONI test results indicate that a multitude of blogs, both local and foreign, are blocked in Iran. For instance, in March 2011 the popular platforms Blogger and Wordpress were blocked in their entirety. According to a senior official at the Ministry of Culture and Islamic Guidance's Center for Information Technology and Digital Media, the decision to block such platforms was made to increase the use of Iranian user-centric websites, and also to combat ideological and political threats.[19] Iranian platforms are as popular as foreign ones among Iranian bloggers, especially Blogfa. However, the platform was filtered in May 2010, after which its owner, Alireza Shirazi, was arrested. Today, Blogfa is no longer filtered and remains a popular blogging platform among Iranians.[20]

Prominent political figures have also been subject to censorship. In December 2011, the website of former president Ayatollah Hashemi Rafsanjani was taken down by its host AfraNet.[21] According to Mr. Rafsanjani's head of office, the website's management received an e-mail from a group named Website Monitoring Group that asked for the text of Mr. Rafsanjani's latest Friday prayer sermons to be removed from his website.[22] The management's failure to comply with the monitoring group's demand resulted in the website being taken down. According to Rafsanjani's office manager, the source of this order was not clear.

Over the years, especially with the creation of the Working Group to Determine Instances of Criminal Content Online and the establishment of the www.samandehi.ir website, the filtering process has become more systematic and uniform. According to officials, only content that the working group deems to be against national beliefs and safety is to be filtered without warning.[23] The Iranian government further legitimizes its heavy filtering by invoking notions of "lawfulness" and social welfare. As www.peyvandha.ir states on its survey of world filtering practices:

> In our country also, the necessity of organized and regulated filtering is greatly felt. Unlimited access should not be given to all segments of society to access the unlimited and borderless world of the Internet. This uncontrolled access is the starting point of damages and pests which, in the twenty-first century and in the age of modern media, affect

[18] John Kelly and Bruce Etling, "Mapping Iran's Online Public: Politics and Culture in the Persian Blogosphere," Berkman Center for Internet and Society at Harvard University, 5 April 2008, http://cyber.law.harvard.edu/publications/2008/Mapping_Irans_Online_Public (accessed 7 November 2012).

[19] "A 'Robot' for Analyzing the Persian Blogosphere," *Global Voices*, 19 January 2008. http://globalvoicesonline.org/2008/01/19/a-robot-for-analyzing-the-persian-blogosphere (accessed 24 October 2012).

[20] "Iran: Head of a Leading Blog Provider Service Arrested," *Global Voices*, 13 May 2010, http://globalvoicesonline.org/2010/05/13/iran-head-of-a-leading-blog-provider-service-arrested (accessed 24 October 2012).

[21] "What Was the Reason for Blocking the Website of the Chairman of the Expediency Council?" [in Farsi] *Aftab News*, 30 December 30 2011, http://aftabnews.ir/vdcbw5b8wrhba8p.uiur.html (accessed 22 April 2012).

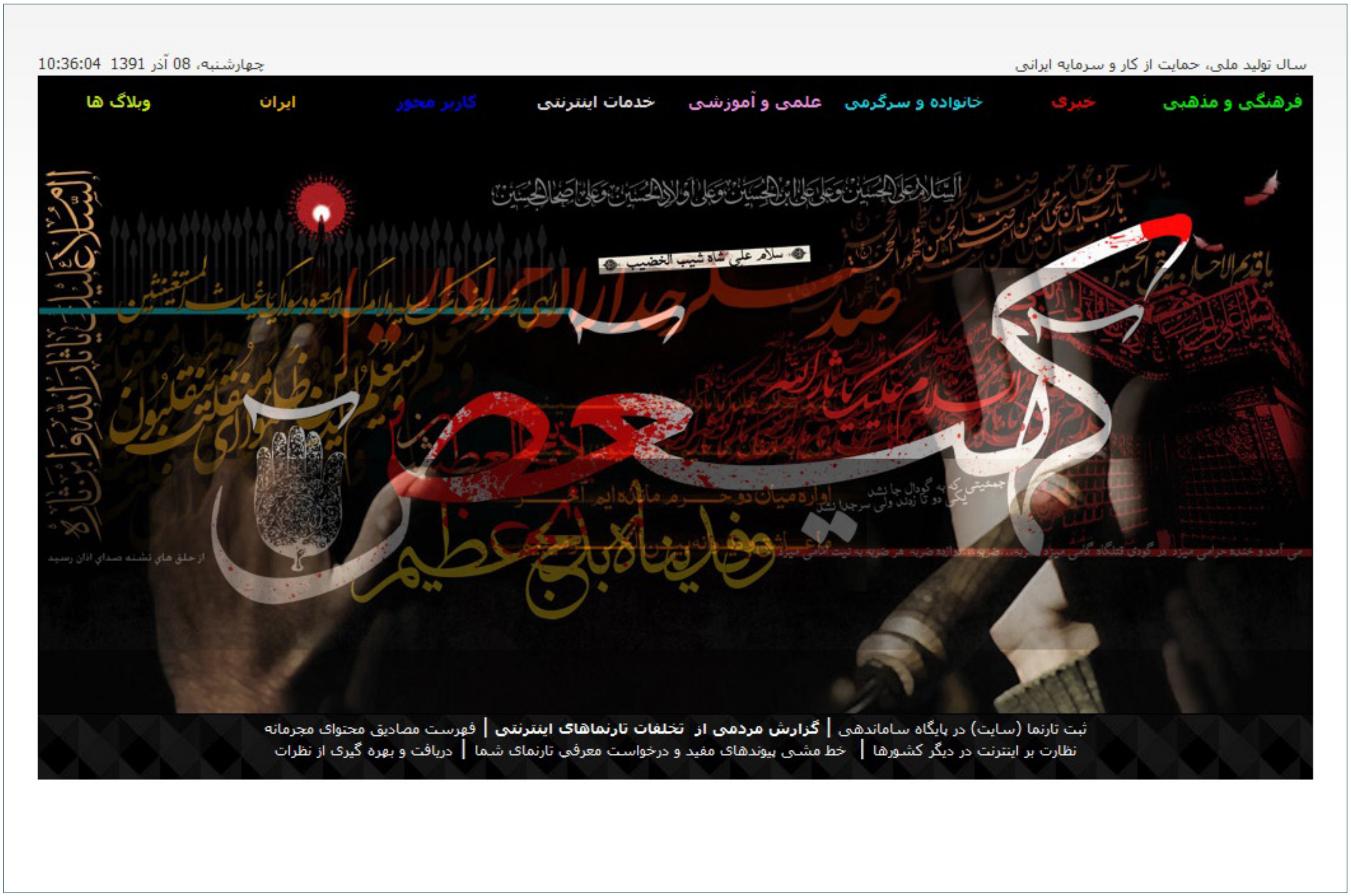
[22] "Iran ex-President Rafsanjani's Website Blocked," *BBC News*, 30 December2011, http://www.bbc.co.uk/news/world-middle-east-16368472 (accessed 23 March 2012).

[23] "Momen Nesab: Filtering in Iran is Completely Democratic," [in Farsi] *Nedaye Enghelab News Agency*, 10 March 2012, http://www.nedayeenghelab.com/vdcirzap.t1awv2bcct.html (accessed 22 April 2012).

> children and youth more than anyone else by targeting their peace of mind and mental well-being. Organized and regulated filtering, to purify the cyberspace environment and protect the society's peace of mind, is not just an option but a necessity.[24]

During testing, ONI discovered that the Iranian filtration system distinguished between sites that were blacklisted due to their content and those that were filtered for containing banned words. However, when Iranian users attempt to access a filtered site, the block page at which they arrive does not list criteria for filtering. Regardless of the nature of the site that is to be accessed, users in Iran are directed to an "Access Denied" page that reads: "In reference to the Cyber Crimes Law, access to the requested website is not possible." This page, www.peyvandha.ir, includes a list of government-recommended websites that are arranged into the following categories: "culture and religion," "news," "family and entertainment," "education and science," "Internet services," "user-centric media," and "Iran." Those whose websites have been blocked may appeal through www.samandehi.ir, a website introduced in July 2011 by the Ministry of Culture and Islamic Guidance.

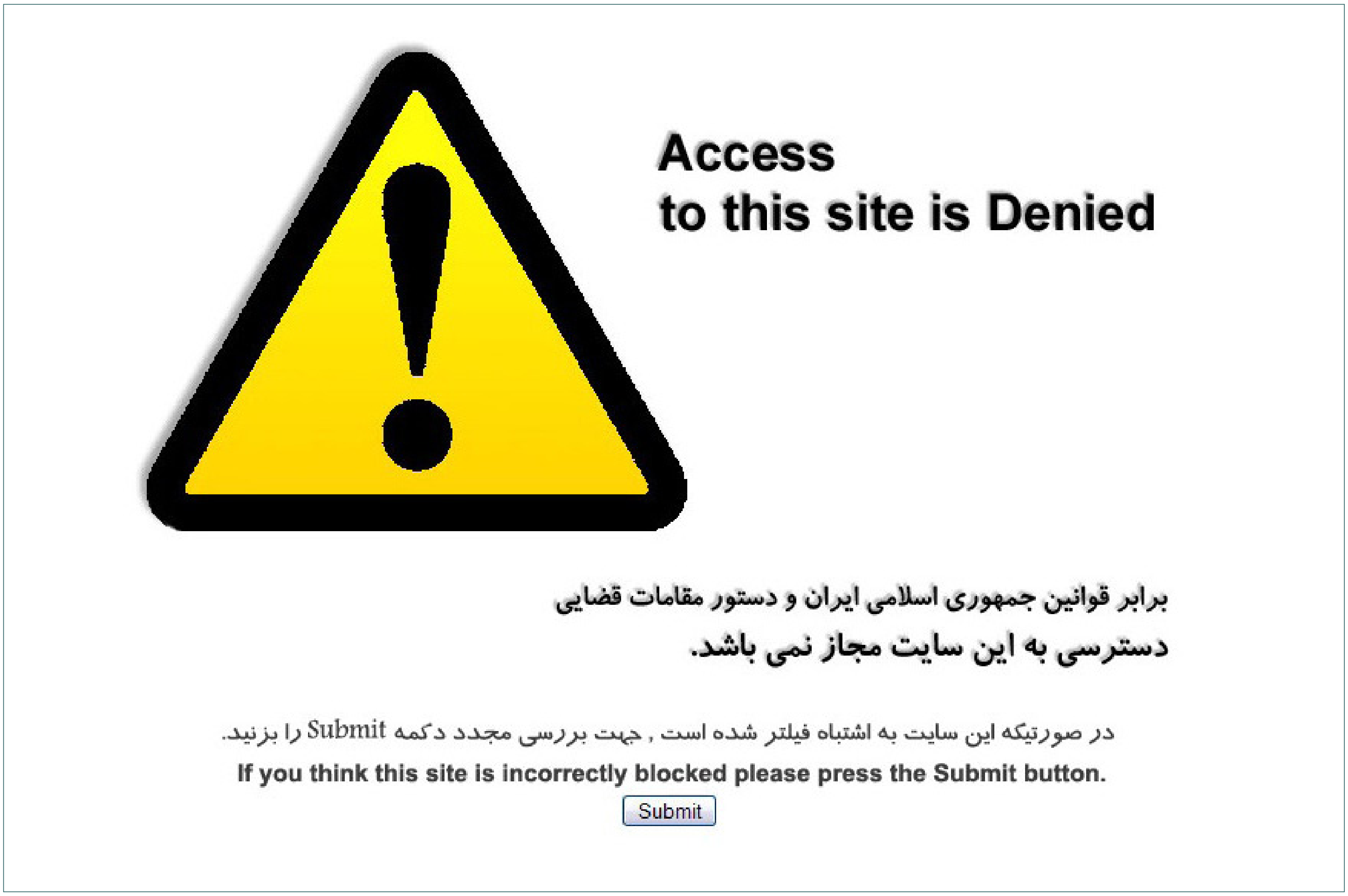
FIGURE 2: IRAN'S NEW "ACCESS DENIED" PAGE (PEYVANDHA.IR) WITH THE LIST OF GOVERNMENT RECOMMENDED WEBSITES.



سال تولید ملی، حمایت از کار و سرمایه ایرانی
چهارشنبه، 08 آذر 1391 10:36:04
فرهنگی و مذهبی
خبری
خانواده و سرگرمی
علمی و آموزشی
خدمات اینترنتی
کاربر محور
ایران
وبلاگ ها
ثبت تارنما (سایت) در پایگاه ساماندهی | گزارش مردمی از تخلفات تارنماهای اینترنتی | فهرست مصادیق محتوای مجرمانه
نظارت بر اینترنت در دیگر کشورها | خط مشی پیوندهای مفید و درخواست معرفی تارنمای شما | دریافت و بهره گیری از نظرات

[24] "Filtering and Monitoring of the Internet in Countries around the World," [in Farsi] *Peyvandha*, http://peyvandha.ir/0-5.htm (accesed 25 October 2012).

FIGURE 3: THE ORIGINAL “ACCESS DENIED” MESSAGE USERS ENCOUNTERED WHEN THEY ATTEMPTED TO ACCESS FILTERED WEBSITES.



Access
to this site is Denied

برابر قوانین جمهوری اسلامی ایران و دستور مقامات قضایی
دسترسی به این سایت مجاز نمی باشد.

در صورتیکه این سایت به اشتباه فیلتر شده است , جهت بررسی مجدد دکمه Submit را بزنید.

If you think this site is incorrectly blocked please press the Submit button.

Despite attempts to systematize censorship, filtering has been sporadic at times. For several hours on 11 July 2011, Iranians had access to a completely unfiltered Internet while authorities were reportedly upgrading the country’s filtering system.[25] Additionally, the *https* protocol was blocked for only a short time leading up to Iran’s parliamentary elections in February 2012. During this period, websites using SSL encryption (including all major foreign e-mail services such as Hotmail, Yahoo, Gmail, etc.) were found to be inaccessible in Iran and those circumvention tools that relied on the *https* protocol were rendered useless. Some reports indicated that SSL-secured sites hosted in Iran were accessible, while those hosted outside the country were effectively blocked.[26] While this blocking lasted only until the end of February, it gives sufficient evidence that Iranian authorities have the capability to shut off usage of foreign e-mail services, possibly as a means to encourage the use of native services. Similarly, in September 2011, following a comment from the Minister

[25] Saeed Kamali Dehghan, “Iran tightens online censorship to counter US ‘shadow internet’,” *The Guardian*, 13 July 2011, http://www.guardian.co.uk/world/2011/jul/13/iran-tightens-online-censorship (accessed November 28, 2012).

[26] Gregg Keizer, “Iran Blocks Access to Some Outside Websites, Services,” *Computer World*, 10 February 2012, http://www.computerworld.com/s/article/9224182/Iran_blocks_access_to_some_outside_websites_services (accessed October 24, 2012).

of Communications on the illegality of VPN use, the PPTP protocol was blocked in its entirety. However, shortly thereafter access to VPNs was restored.[27]

INTERNET CAFÉ LAWS

In January 2012, Iran's Internet Police (FETA) announced new regulations that were to be implemented immediately for Internet cafés. Under the new regulations, Internet cafés must equip their facilities with cameras and register their customers' information.[28] Café owners are required to record users' names, numbers, national identification numbers, post codes, and telephone numbers, as well as the date, time, IP address, and website addresses they visit.[29] The new guidelines also specifically ban the installation and use of circumvention tools and VPNs on Internet café computers.[30] The extent to which these regulations have been reinforced is not yet known.

[27] "ISNA Reports: VPN Tunnels Blocked Due to Criminal Use," [in Farsi] Iranian Students' *News Agency*, 3 October 2011, http://old.isna.ir/ISNA/NewsView.aspx?ID=News-1860740 (accessed 25 October 2012).

[28] Farnaz Fassihi, "Iran Mounts New Web Crackdown," *The Wall Street Journal*, 6 January 2012, http://online.wsj.com/article/SB10001424052970203513604577142713916386248.html (accessed 20 November 2012).

[29] Saeed Kamali Dehghan, "Iran Clamps Down on Internet Use," *The Guardian*, 5 January 2012, http://www.guardian.co.uk/world/2012/jan/05/iran-clamps-down-internet-use (accessed 24 October 2012).

[30] "FETA's Ultimatum to Internet Café Owners," [in Farsi] Iranian Students' *News Agency*, 3 January 2012, http://isna.ir/ISNA/NewsView.aspx?ID=News-1923707 (accessed 4 April 2012).

BEYOND FILTERING: LEGAL AND REGULATORY INSTITUTIONS

The "Green Movement" exposed the shortcomings of rudimentary filtering tools, which were unable to prevent online mobilization and communication, and drove the Iranian regime to adopt more complex methods. Since 2009, the government has increasingly emphasized nontechnical mechanisms of control. It has not only passed legislation that specifically targets and criminalizes certain forms of online activity, but has also pursued a comprehensive bureaucratization of cyberspace, subsuming regulatory functions under myriad government entities. At the same time, there have been multiple instances of advanced filtering techniques, including selective protocol blocking.

FREEDOM OF SPEECH

Freedom of speech holds a contentious position within the Iranian constitution and other relevant legislation, the most notable of which are the country's Press Law and Cyber Crimes Law. On the subject of freedom of speech, many legal scholars cite articles 23 and 25 of the Iranian constitution as points of reference. In particular, article 23 outlines that the "inquisition of an individual's beliefs is illegal, and no one can be attacked or taken to task for their belief." Article 25 also states that "inspection, and sending of letters, disclosing and recording of telephone conversations, or disclosure of telegraphic and telex communications, censorship, the willful failure in their transmission, eavesdropping, and any form of surveillance is prohibited, unless stated by the rule of law."[31]

Based on Iranian jurisprudence, the prohibition of surveillance can be inferred as a principle. However, certain cases, which often revolve around concerns like conspiracy against Muslims and Islam or the endangerment of the population and personal property, can be considered necessary exceptions to this rule. In such cases protecting the agency, security, and tranquility of Iran's Islamic society and the ruling system supersedes the rights of the individual. Thus, according to those pretexts, surveillance may be conducted when the nation is considered under threat.

Legal exceptions to the prohibition of surveillance are elaborated in the Press Law of 1986, which is the primary mechanism through which the government regulates Iranian media. Article 6 of the Press Law and its twelve subsections outline broad restrictions on freedom of speech. These include:

> the prohibition to "promote subjects who might damage the foundation of the Islamic Republic, … offending the Leader of the Revolution, … publishing libel against officials,… encouraging and instigating individuals and groups

[31] Constitution of the Islamic Republic of Iran, adopted 23 October 1979, amended 28 July 1989, articles 23 and 25.

> to act against the security, dignity, and interests of the Islamic Republic of Iran within or outside the country, … [and] publishing anything critical of the constitution.[32]

The Press Law was amended twice in 2000 and 2009 in order to bring electronic publications and online content sources under its purview.[33] "Internet publications" are required under the law to obtain a licence or else face prosecution under the country's harsh Penal Code.[34] The law's broad scope and ambiguous wording have provided Iranian authorities with legal power to arrest bloggers and journalists and to restrict freedom of expression on the Internet.

For this reason, the Committee to Protect Journalists has ranked Iran as the second-worst country for bloggers in the world.[35] Hossein Derakhshan, also known as the "father of Iranian blogging," was arrested in October 2008, and later sentenced to nineteen and a half years in prison under the charges of "co-operating with hostile states," "propaganda against the regime," and "creating and overseeing vulgar and obscene websites." Derakhshan, a dual citizen of Iran and Canada, is best known for his advocacy on the use of the Internet to bring about social and political reform.[36] Hossein Ronaghi-Maleki, the blogger and activist who wrote under the pen name Babak Khorramdin, was arrested in December 2009, charged with "accepting money from Western countries," "helping political prisoners escape Iran," and "heading political gangs." Mr. Ronaghi-Maleki is currently suffering from severe kidney conditions while he serves his prison sentence.[37] In March 2009, blogger Omidreza Mirseyfi died under suspicious conditions in Evin prison while serving his thirty-month sentence. Mirseyfi was accused of insulting the leaders of Iran's Islamic revolution in his writings. His death was reported as a suicide.[38]

THE CYBER CRIMES LAW

Iran's "Cyber Crimes Law" has provided the state a far greater level of control over Internet legislation than has the Press Law.[39] It gives government the purview to determine what is considered legal or illegal, and allows the authorities to punish those who break the rules by imprisonment and fine. The law was first ratified by the Iranian parliament on 17 November 2008 and was subsequently approved by the Guardian Council on 28 June 2009, only sixteen days after the disputed presidential election of

[32] Press Law, ratified on 19 March 1986, amended on 18 April 2000, article 6.

[33] "Iran" in *Access Controlled*, 549-50

[34] Ibid.

[35] "Ten Worst Countries to Be a Blogger," *Committee to Protect Journalists*, 30 April 2009, http://cpj.org/reports/2009/04/10-worst-countries-to-be-a-blogger.php (accessed 20 March 2012).

[36] Mike Butcher, "The 'Father' of Iranian Blogging, Jailed for Nineteen Years, Reappears on Facebook." *TechCrunch*, 6 May 2011, http://techcrunch.com/2011/05/06/the-father-of-iranian-blogging-jailed-for-19-years-reappears-on-facebook/ (accessed 25 March 2012).

[37] "'My Son Is Under Pressure to Participate in Televised Confessions,' Says Activist's Mother," International Campaign for Human Rights in Iran, 6 August 2010, http://www.iranhumanrights.org/2010/08/son-pressured-confession/ (accessed 23 March 2012); "Blogger Returned to Prison Two Days After Surgery," *International Campaign for Human Rights in Iran*, 30 January 2012, http://www.iranhumanrights.org/2012/01/ronaghi-surger/ (accessed 16 March 2012).

[38] "Blogger Dies in Iran's Evin Prison," Committee to Protect Journalists, 19 May 2009, http://cpj.org/2009/03/blogger-jailed-for-insulting-leaders-dies-in-irans.php (accessed 16 March 2012).

[39] Islamic Republic of Iran: Computer Crimes Law. Available at http://www.article19.org/data/files/medialibrary/2921/12-01-30-FINAL-iran-WEB[4].pdf (accessed 27 August 2012). We translate as "Cyber Crimes Law."

12 June 2009.[40] The timing of the legislation, coinciding with escalating anti-government protests and online opposition, seems to indicate that it was a direct reaction to the shortcomings of existing legal statutes and regulatory bodies. Three important aspects of this law are most relevant: 1) it creates a centralized Internet censorship body with legal power, 2) it obliges ISPs to cooperate with the government in filtering and surveillance, and 3) it criminalizes access to banned websites either directly or by use of circumvention tools.

The Cyber Crimes Law gave rise to the establishment of a new centralized censorship body called the Working Group to Determine Instances of Online Criminal Content. According to article 22, the Ministry of Justice is responsible for establishing the working group—an interagency body that has legal powers, and makes final decisions about Internet filtering. Members of the working group include: ministers or representatives from the Ministries of Education, Information Communication Technology (MICT), Intelligence, Justice, Science, Research and Technology, Culture and Islamic Guidance; the head of the Islamic Propagation Organization; the head of Islamic Republic of Iran Broadcasting (IRIB); the commander of the police forces; an ICT expert recommended by parliament; and a representative from the parliament's judiciary committee.[41] The members are led by Iran's Prosecutor General. The working group is part of the judiciary branch of the government, and its decisions are deemed legally binding. According to the Cyber Crimes Law, however, all three branches of government — the executive, parliamentary, and judiciary — are obliged to be involved in Internet censorship.[42] Iran's Telecommunication Infrastructure Company (TIC), which works under the Ministry of Information Communication Technology (MICT), is in turn responsible for implementing the decisions of the working group. If the working group deems the content of a website "criminal," it informs the TIC, which in turn instructs the Telecommunication Company of Iran (TCI) to block access to the website through the country's ISPs.[43] The Cyber Crimes Law obliges ISPs to cooperate with the government in both Internet filtering and surveillance. Article 23 of the Cyber Crimes Law states that ISPs should be held responsible for blocking access to criminal content as determined by the working group. Article 32 further mandates that ISPs must maintain traffic data for a minimum of six months after its collection. Traffic data is here defined as "any data that the computer system produces through a chain of computer communication and telecommunication," including information such as origin, route, date, time, duration and volume of communication and type of services. Iranian ISPs must also save the personal information of their users for a minimum of six months after the cancellation of subscriptions, including identity, geographic addresses, IP addresses, and telephone numbers.[44]

None of the articles in the Cyber Crimes Law

[40] "Iran's Cyberspace Criminal Law Was Announced," [in Farsi] *Khabar Online*, 13 July 2009, http://www.khabaronline.ir/news-12548.aspx (accessed 26 February 2010).

[41] "About Us," The Working Group to Determin Instances on Online Criminal Content, http://internet.ir/aboutus.html (accessed 23 November 2012)

[42] "History and Introduction to the Working Group," The Working Group to Determine Instances on Online Criminal Content, http://internet.ir/intro.html (accessed 23 November 2012)

[43] Ibid.

[44] Computer Crimes Law.

itself declare the use of VPNs and circumvention tools to be criminal. However, the ambiguity of articles 1 and 25 allows for different interpretations of the illegality and criminality of VPN and circumvention tool usage. These two articles refer to the protection of data through "secure measures," and state that "unauthorized access" to such data is punishable by law. Experts believe that these articles criminalize hacking and that the phrase *secure measures* does not refer to circumvention tools or VPNs. Others, however, contend that the concept of "unauthorized access" in these articles refers to access through circumvention tools, which in turn renders their use illegal.[45] Regardless of the finer points of legal interpretation, the Minister of Communication and the Working Group for Determining Instances of Online Criminal Content have clearly announced that the use of circumvention tools and VPNs is illegal.[46] This determination necessitates that "unauthorized access" as referred to in articles 1 and 25 be defined as any sort of bypassing of government-implemented filters. Still, some government officials have publicly declared that the use of VPNs is not illegal, especially since the Cyber Crimes Law does not outline the VPN protocol's criminality.[47]

So far, there have been no reports on any case of conviction by law based on the use of VPNs and circumvention tools. In the past, however, the authorities have announced the arrest of people who were involved in the "production and propagation of circumvention tools" that helped people to bypass Internet filters.[48] *Kayhan Newspaper*, which has close ties to Iran's intelligence agencies, has reported that a network under the name "Iran Proxy" had distributed over 70 million circumvention tools by early 2010.[49] Furthermore, in a televised interview on Iran's national TV, a representative of the IRGC's Cyber Defence Command, Gerdab.ir, mentioned that one of the "criminal" activities of "Iran Proxy" was "creating a safe platform to send news to Western countries, and radio and television networks such as *Radio Zamaneh*, *Radio Farda*, and the Television Network of the USA [*Voice of America*] (*VOA*)."[50]

THE SUPREME COUNCIL ON CYBERSPACE

On 7 March 2012, Supreme Leader Ayatollah Khamenei decreed the creation of the Supreme Council on Cyberspace, to be headed by President Mahmoud Ahmadinejad.[51] The move indicates the increasing importance that the Internet holds to the Iranian government and its perceived

[45] Mostafa Tok Hamedani, "What Law Criminalizes the Use of Circumvention Tools?," Iranian Journalists, 21 November 2011, http://khabarnegaran.info/article.php3?id_article=473 (accessed 26 November 2012) and "A Legal Battle About VPN," Virtual Society of Iranian Lawyers, 18 October 2011, bit.ly/TpmSa0 (accessed 26 November 2012)

[46] Golnaz Esfandiari, "Are Millions of Iranians Criminals?" *Radio Free Europe Radio Liberty*, 25 October 2011, http://www.rferl.org/content/iran_internet_antifiltering_tools_censorship/24370376.html (accessed 20 November 2012)

[47] "Instances of Computer Crimes for the Use of Email and VPNs," *Mehr News*, 20 February 2012, http://www.mehrnews.com/fa/newsdetail.aspx?NewsID=153531 (accessed 20 March 2012).

[48] "New Details About Destruction of the CIA Cyberspace Network," [in Farsi] *Kayhan Newspaper*, 15 March 2010, http://www.kayhannews.ir/881224/2.htm#other201 (accessed 15 March 2010).

[49] Ibid.

[50] "Details About Arresting Members of Cyberspace War," [in Farsi] *Tabnak News Agency*, 15 March 2010, http://www.tabnak.ir/fa/pages/?cid=90171 (accessed 16 March 2010).

[51] "Leader Decrees Establishment of Supreme Council of Cyberspace," *PressTV*, 7 March 2012, http://www.presstv.ir/detail/230425.html (accessed 24 October 2012).

need to centrally control information flows.

The Farsi Language website of Ayatollah Khamenei provides an outline of the council's function, members, and goals.[52] It explains that the new council will consist of a number of "legal members"—Iran's highest-ranking officials —and seven "natural persons." The legal members include the president, Majlis Speaker, Judiciary Chief, director of the IRIB (Islamic Republic of Iran Broadcasting), secretary of the Supreme National Security Council, Minister of IT and Communications, Minister of Culture and Islamic Guidance, Minister of Sciences, Research, and Technology, commander of the IRGC, and the national police chief. The "natural persons" are technology experts, engineers, directors of media outlets like Press TV, directors of the IRIB, and a few people closely affiliated with the Supreme Leader.[53]

Ayatollah Khamenei claims that the council was established due to the increasingly important roles that information technology, the communications sector, and the global Internet play in the personal and social dimensions of individuals' lives. Khamenei further highlights the need for "targeted and extensive investment in the field" in order to maximize the "opportunities that arise from this sector for the development of the country." He also emphasizes the "importance of continuous planning and coordination, in order to protect against [cyberspace's] harms." By creating a centralized system of "policy-making, decision making and coordination," Khamenei believes that Iran will acquire a robust cyber defence.[54]

The Supreme Council's activities began in earnest in late June 2012. At a press conference, Mehdi Akhavan Behabadi, the recently appointed secretary general of the Supreme Council on Cyberspace and director of the National Centre for Cyberspace, stated that the organization would not play a direct role in filtering.[55] Rather, he argued that the Supreme Council would be responsible for making decisions regarding the current state of the country's cyberspace devices, coordinating other institutions, and monitoring the Internet for overall performance. Another Iranian official, Saeed Salarian, reported that the body will review government websites and develop standardized templates to be followed in the future. The secretary general later commented on the successful transfer of government websites to local hosts, noting that a domestic market for private-sector hosting of government data should be developed.[56] The Supreme Council's evident interest in the overall infrastructure of cyberspace, in formatting official websites, and in promoting Iranian domain names seems to indicate that it will have an important role in the development of a standardized "National Internet" for Iran.

[52] "Order for the Creation of the Supreme Council on Cyberspace," [in Farsi] *Ayatollah Khamenei Official Website*, http://farsi.khamenei.ir/ndata/news/19226/901217majazi.pdf, 7 March 2012 (accessed 4 April 2012).

[53] "Background and Education of the Natural Members of the Supreme Council on Cyberspace," [in Farsi] *Weblog News*, 7 March 2012, http://weblognews.ir/1390/12/forms/news/19383/ (accessed 3 April 2012).

[54] "Formation of the Supreme Council on Cyberspace and the Appointment of Its Natural and Legal Members," [in Farsi] *Ayatollah Khamenei Official Website*, 7 March 2012, http://farsi.khamenei.ir/message-content?id=19225 (accessed 4 April 2012).

[55] "The Supreme Council of Cyberspace's Plan for National Internet: Licensing System for Virtual Activities," [in Farsi] *Mehr News*, 26 June 2012, http://www.mehrnews.com/fa/newsdetail.aspx?NewsID=1635832.

[56] "Criticism of State Internet Tools: Reform of IT Policies," [in Farsi] *Mehr News*, 10 July 2012, http://www.mehrnews.com/fa/newsdetail.aspx?NewsID=1646674

OTHER REGULATORY BODIES

There are a number of other institutions involved in Internet regulation in Iran, many of which appear to have overlapping responsibilities. Iran's Intelligence Ministry is active in monitoring the Internet and arresting "cyber criminals."[57] An additional authority, the Information Communication Technology Section of Iran's Police Forces (FAVA/ICT Police), has offices in different provinces and a budget of 90 million US dollars—according to Iran's Commander of Police Forces, Esmail Ahmadi Moghadam—to monitor the Internet.[58]

The Islamic Revolutionary Guard Corps (IRGC) is also increasingly involved in blocking access to so-called criminal content on the Internet. IRGC's Cyber Defence Command, Gerdab.ir, is in charge of dealing with organized cybercrime, including terrorism, spying, and economic and social crimes.[59] The IRGC reportedly also recruits and trains thousands of "cybersoldiers" to monitor the online activity of dissidents, post propaganda on blogs and forums, and report to various state bodies.[60] In March 2010, Fars News Agency reported that IRGC's Cyber Defence Command "destroyed" twenty-nine cyberspace "spying" websites that belonged to Iran's Human Rights Activists News Agency.[61] The hacked websites had supposedly "acted against Iran's national security under the cover of human rights activities."[62]

FETA (Cyber and Information Exchange Police), is yet another mechanism for monitoring cyber crimes. With offices in every province of the country, it was established on 19 April 2011 with the mission to identify "new crimes against the people's safety, the moral domain, economic and even terrorist activities."[63]

The Passive Defence Organization (PDO) has also played a key role in combating Internet-based threats to the regime since the unrest in 2009. The PDO was established in 2002-2003 by the order of the Supreme Leader, Ayatollah Ali Khamenei, under the direct supervision of the Iranian Armed Forces. The organization is made up of nine departments and its structure is directly approved by the Supreme Leader himself.[64] Brigadier General Gholamreza Jalali, the director of the PDO, defines the organization's activities as aiming to decrease national vulnerabilities, while increasing stability against foreign threats without the use of arms. The PDO identified the post-election protests as an event that exposed the country's weaknesses in the field of

[57] "Many Centres, Groups, and Organizations, Just to Control the Internet," [in Farsi] *Radio Farda*, 15 February 2010, http://www.radiofarda.com/content/f35_Iran_Internet_Under_Control/1958457.html (accessed 26 February 2010).

[58] Ibid.

[59] "About Us," [in Farsi] *Gerdab*, http://www.gerdab.ir/fa/about (accessed 25 October 2012).

[60] Farnaz Fassihi, "Iran's Censors Tighten Grip." *The Wall Street Journal*, 16 March 2012, http://online.wsj.com/article/SB10001424052702303717304577279381130395906.html (accessed 24 October 2012).

[61] "IRGC's Cyber Department Hacks Twenty-nine US-Backed Websites," *Fars News Agency*, 14 March 2010, http://english.farsnews.com/newstext.php?nn=8812231183 (accessed 24 October 2012).

[62] Ibid.

[63] Ahmadi Moqaddam and Farmandeh Naja, "'Anti-Cybercrime' Police Established in Every Province," [in Farsi] *Weblog News* 19 April 2011, http://weblognews.ir/?p=13985 (accessed 25 October 2012).

[64] "Everything About the Civil Defence Organization," *Iran Newspaper on Network*, 10 October 2010, http://www.inn.ir/newsdetail.aspx?id=59182 (accessed 3 April 2012).

civil defence.[65] In November 2011, General Jalali announced that he had received direct orders from the Supreme Leader to set up a cyber defence base for Iran. According to him, the cyber-defence base will trace the cyber threats that are posed against the infrastructure of the country's national security. General Jalali later identified cyber security as a policy priority for all government agencies and ministries, particularly the ministries of Intelligence, IT and Communications, Defence, and the PDO itself.[66]

[65] Official Website of Passive Defence Organization [in Farsi], http://www.paydarymelli.ir/ (accessed 1 April 2012).

[66] Hamed Shafi'i, "Cyber Defence Base Was Established," [in Farsi] Shargh Newspaper, 2 November 2011, http://sharghnewspaper.ir/News/90/08/11/15786.html (accessed 4 April 2012).

TOWARD A NATIONAL INTERNET: INFORMATION CONTROL

While enacting considerable changes to Iran's legal and regulatory environment, the government has also begun to pursue more complex techniques of control. Rather than simply censor content by denying Iranians access to certain websites or blacklisting specific keywords, the regime has increasingly sought to compete in cyberspace with the West and with domestic dissidents by waging an information war. Considerable effort has been directed toward "building new pro-government virtual spaces wherein the official culture could be propagated, made visible and, accordingly, legitimize state power."[67] New initiatives have focused on creating a distinctly "Iranian" Internet and engendering a climate of self-censorship through a number of mechanisms. The newly developed "National Information Network" will erect state-defined boundaries to accessing content, while facilitating government surveillance of those who remain on the Internet. The regime has encouraged the actions of "Internet brigades," groups of loosely affiliated hacktivists who use disinformation, propaganda, and harassment to "effect cognitive change" in society.[68] The state has also embraced social-media tools at the highest levels. Ayatollah Khamenei now has accounts on Twitter[69] and Instagram[70] through which he posts updates for the Iranian population and diaspora.

IRAN'S NATIONAL INFORMATION NETWORK

Inspired by Chinese efforts to control the World Wide Web and create a *de facto* "domestic" Internet,[71] the Iranian government declared its intention to create a national intranet in April 2011. In a speech, Iranian Deputy Minister for Economic Affairs Ali Agha Mohammadi openly said that "Iran will soon create an internet [sic] that conforms to Islamic principles, to improve its communication and trade links with the world... We can describe it as a genuinely 'halal' network aimed at

[67] Babak Rahimi, "The Agonistic Social Media: Cyberspace in the Formation of Dissent and Consolidation of State Power in Postelection Iran," *The Communication Review*, 14 no. 3 (2011): 170. http://www.tandfonline.com/doi/pdf/10.1080/10714421.2011.597240 (accessed 24 October 2012)

[68] Deibert and Rohozinski, "Control and Subversion," 28

[69] The Centre for Preserving and Publishing the Works of Grand Ayatollah Sayyid Ali Khamenei, khamenei.ir. Available at: https://twitter.com/khamenei_ir.

[70] "Picture This: Iran's Ayatollah Khamenei Joins Instagram," *Al Arabiya News*, 4 August 2012, http://english.alarabiya.net/articles/2012/08/04/230309.html (accessed 24 October 2012).

[71] Neal Ungerleider, "Iran Cracking Down Online with 'Halal Internet,'" *Fast Company*, 18 April 2011, http://www.fastcompany.com/1748123/iran-launching-halal-internet (accessed 24 October 2012).

Muslims on a ethical and moral level."[72] Minister Mohammadi envisioned that the creation of such a domestic intranet would take eighteen months and would be developed with the assistance of "foreign consultants."[73]

Iran has reportedly been developing its "National Information Network" since 2005 and had initially planned to launch the project by the end of 2009.[74] The plan for this network was mentioned in article 49 of Iran's Fifth Economic Development Plan (2010-2015), which stated that Iran should aim for a functional version by 2015. According to this article, the Ministry of Communications and Information Technology is responsible for expanding the services of the e-government and increasing productivity in the economic, social, and cultural sectors through the sustainable and safe development of a "National Information Network."[75] The network would look similar to the global Internet, but content from and contact with the World Wide Web would be restricted or subject to heavy government control. The goal is to create a system that no longer requires Iranian Internet traffic to be routed through external (often US-based) servers that expose data to interception.

Toward this end, the government recently initiated a transfer of all government website domains to local hosts and inaugurated the National Science and National School Network, leading some to believe that the full implementation of the National Information Network is imminent.[76] A test version of the network was launched in Qom in January 2010. Since this announcement, there have been indications that, at the very least, the Iranian government has tried to encourage a nationalization of Iranian users' online experience. In May 2012, Minister of Communications Reza Taqipour declared that mobile telephone companies would be prohibited from sending statements to clients using foreign e-mail services.[77] Executive and academic institutions were also required to have ".ir" top-level domain extensions for their websites.[78]

In late September 2012, Deputy Communications and Technology Minister Ali Hakim-Javadi confirmed that the first phase of implementing Iran's National Information Network had been completed.[79] All government ministries and organizations are connected to Iran's intranet, with full domestic integration slated for completion by March 2013. In tandem with this announcement, state media announced that Google-affiliated services would be banned until further notice. ONI attempted to access Google through two Iranian ISPs—Kara Amin Ertebat and Information Technology Company —and

[72] "Iran: Tehran Announces New 'Halal' Islamic Internet," *ADN Kronos International*, 15 April 2011, http://www.adnkronos.com/IGN/Aki/English/CultureAndMedia/Iran-Tehran-announces-new-halal-Islamic-internet_311908244227.html.

[73] "Iran Cracking Down Online."

[74] Khashayar Nouri, "Tehran's Unplugged Internet Plan," *Payvand Iran News*, 23 October 2010, http://www.payvand.com/news/10/oct/1189.html (accessed 24 October 2012).

[75] "Fifth Economic Development Plan: Complete Information on the Plan/Bill," [in Farsi] *Majlis Research Center*, http://rc.majlis.ir/fa/legal_draft/show/771977 (accessed 1 April 2012).

[76] "Immigrants Are Filtered," [in Farsi] *GERDAB News Archives*, 14 July 2010, http://bit.ly/HUUpjV (accessed 2 April 2012).

[77] "New Restriction on the Use of Foreign E-mail," *IT Analyze*, 11 May 2012, http://itanalyze.com/news/2012/05/11/17594.php (accessed 25 October 2012).

[78] "National E-mail: Fraught with Ambiguity," *IT Analyze*, 12 May 2012, http://itna.ir/vdcc0sqi.2bqi08laa2.html (accessed 25 October 2012).

[79] "Iran Readies Domestic Internet System, Blocks Google," *Reuters*, 23 September 2012, http://ca.reuters.com/article/technologyNews/idCABRE88M0AO20120923?pageNumber=1&virtualBrandChannel=0 (accessed 24 October 2012).

notably received an error message rather than a typical blockpage. However, many people inside Iran—including several members of parliament—responded negatively to the filtration of Gmail, and Google services were subsequently unblocked.[80] In October 2012, Collin Anderson reported that Iran has made a significant step toward creating a "private network [that] is accessible [only] to a wide section of the nation's Internet users" and that a number of ISPs and government organizations have purposefully sought "to adopt the use of private [IP] addresses across networks."[81] However, the presence of a private network, which corroborates with the statements of Iranian officials, does not necessarily augur total disconnection from the Internet.

Despite fears of an actual separation between Iran and the World Wide Web, the government has denied that the National Information Network will serve as a replacement for the Internet.[82] These assurances aside, foreign influence on Iranian cyberspace is undeniably a concern in government security circles, especially in light of suspected attacks against the country attributed to the United States and Israel. A domestic intranet would offer Iranian authorities better national intelligence and would limit citizens' access to content that authorities deem to be suitable.[83]

The National Information Network bears close resemblance to similar systems in North Korea and Cuba. The North Korean government has developed an isolated intranet consisting of approximately thirty sites called Kwangmyong.[84] The government chooses the content, which is intended primarily for use in libraries, research institutes, and factories. Cuba, by contrast, offers a two-tiered system consisting of the Internet and an intranet.[85] Regulatory measures and cost considerations prevent most citizens from accessing the World Wide Web. Instead, the majority of Cubans connect through RedCubana a walled-off intranet that features national e-mail, government informational websites, and some low-tech Wikipedia and Facebook clones.[86] Cuba's two-tiered system seems similar to what Iran seeks to achieve through the National Information Network: a relatively speedier domestic intranet serving as a practical alternative to a filtered, monitored, and considerably slower global Internet. Nationalism, Western threats of cyberwarfare, and the depiction of major companies such as Google and Facebook as agents of "American soft power" arguably bolster the

[80] Yeganeh Torbati, "Iran Unblocks Gmail After Members Of Iranian Parliament Complain," *The Huffington Post*, 1 October 2012, http://www.huffingtonpost.com/2012/10/01/iran-gmail-blocked_n_1928448.html?utm_hp_ref=technology (accessed 24 October 2012).

[81] Collin Anderson,"The Hidden Internet of Iran Private Address Allocations on a National Network," http://arxiv.org/pdf/1209.6398v1.pdf (accessed 24 October 2012), 1-2.

[82] "Iranians to Remain Connected to World Wide Web," *Payvand Iran News*, 18 January 2012, http://www.payvand.com/news/12/jan/1188.html (accessed 24 October 2012).

[83] "From Halal Internet to Halal Satellite," *Hamshahri-Online*, 24 April 2011, http://www.hamshahrionline.ir/news-133072.aspx [in Farsi] (accessed 15 June 2011); and "Halal Internet in Iran?" [in Farsi] Weblog-News, 19 April 2011, http://weblognews.ir/?p=13981 (accessed 15 June 2011).

[84] "North Korea," *Open Net Initiative*, 10 May 2007, http://opennet.net/research/profiles/north-korea (accessed 24 October 2012).

[85] Abraham Riesman,"Iran's Network in a Bottle," *The Boston Globe*, 15 July 2012, http://www.bostonglobe.com/ideas/2012/07/14/iranian-government-building-internet-all-its-own/60eT7aC7P563vc4ti8auIN/story.html?camp=pm (accessed 24 October 2012).

[86] "Internet Enemies: Cuba," *Reporters Without Borders*, http://en.rsf.org/internet-enemie-cuba,39756.html (accessed 24 October 2012).

authorities' animosity to the Internet.[87]

As in Cuba, Iranian officials have previously cited lower bandwidth costs, better performance, and faster speeds as reasons for developing the National Information Network.[88] However, it is the government itself that limits maximum Internet speeds to 128 kbps, filters websites, and, through its monopoly over ISPs, sets subscription prices. In March 2011, for example, the government announced that provincial telecommunications companies would be increasing the price of high-speed services up to fourteen times for ISPs; this cost would in turn trickle down to the individual user.[89] In preparation for the launch of the national network, it is likely that the Iranian government is pre-emptively encouraging its use by making Internet user experiences as unpleasant and expensive as possible. As the *New York Times* noted, "cutting off all access to the World Wide Web may not even be necessary: It's enough to simply offer a fast, reliable alternative to the usual Iranian Internet experience."[90] Moreover, the government may choose to retain its connections to the Internet, if only as an avenue to survey those citizens who use it instead of the National Network.[91]

[87] Riesman, "Iran's Network."

[88] Nouri, "Tehran's Unplugged Internet Plan."

[89] "Expensive Internet Is on Its Way," [in Farsi] *Hamshahri*, 19 March 2011, http://www.hamshahrionline.ir/news-130780.aspx (accessed 25 October 2012).

[90] Riesman, "Iran's Network."

[91] Alex Meriwether, "Internet Responds to Iran's Rumored 'Halal' Intranet," *Herdict Blog*, http://blogs.law.harvard.edu/herdict/2012/04/19/internet-responds-to-irans-rumored-halal-intranet/ (accessed 24 October 2012).

BOX 2: SURVEILLANCE TOOLS

While the National Information Network is still in development, Iranian cyberspace has recently witnessed complex tools of surveillance emerge. Not all of the examples listed below have been conclusively linked to the state, but they are all instances in which malware or hardware have granted government authorities access to dissidents' personal information.

In July 2011, the Dutch Certificate Authority, DigiNotar, was compromised through what appears to have been a man-in-the-middle (MITM) attack.[1] While the technical details are unclear, it has been reported that over 300,000 Internet users (primarily Iranian) were affected by it. In fact, an Iranian individual has claimed responsibility for the incident. The attack, also referred to as "Operation Black Tulip," reportedly forged SSL certificates for domains belonging to the CIA, MI6, Mossad, and Microsoft among others. Iranian users' Gmail accounts were also targeted.[2] Although no official connections have been found, some believe the person who claimed responsibility for Operation Black Tulip is the same person behind the Comodo attack in early 2011, which involved the theft of multiple SSL certificates belonging to sites like Google, Microsoft, and Skype.[3] Comodo itself issued a statement that it believed the attack was politically motivated and state-sponsored, because the information obtained would allow the perpetrator to "intercept Web-based email/communication and the only way this could be done is if the perpetrator had access to the country's DNS infrastructure."[4] In both the Comodo and Diginotar cases, authorities would be able to use the stolen certificates to trick online activists into believing they were at a legitimate site; in reality, the authorities would be able to collect their usernames and passwords. However, no evidence has been found to suggest any form of state affiliation in either one of these attacks.[5]

In May 2012, the The Citizen Lab uncovered corrupted versions of Simurgh, a popular proxy tool designed to allow anonymous access to blocked websites.[6] The back-doored client installed key-logging spyware and a Trojan that exfiltrates user data to an ISP located in Saudi Arabia. The Trojan was specifically engineered to target Iranians and Syrians attempting to evade government filtering and surveillance efforts, thus raising questions about its creators and their interests.

Nokia-Siemens Networks (NSN), a joint venture between the Finnish cell-phone giant Nokia

[1] Eva Galperin, Schoen Seth, and Eckersley Peter, "A Post Mortem on the Iranian DigiNotar Attack," *Electronic Frontier Foundation*, 13 September 2011, https://www.eff.org/deeplinks/2011/09/post-mortem-iranian-diginotar-attack (accessed 24 October 2012).

[2] Gregg Keizer, "Hackers Steal SSL Certificates for CIA, MI6, Mossad," *Computer World*, 4 September 2011, http://www.computerworld.com/s/article/9219727/Hackers_steal_SSL_certificates_for_CIA_MI6_Mossad (accessed 24 October 2012); Jeremy Kirk, "Google Says Gmail Attack Focused on Iranian Targets," *Computer World*, 30 August 2011, http://www.computerworld.com/s/article/9219582/Google_says_Gmail_attack_focused_on_Iranian_targets (accessed 24 October 2012).

[3] Peter Bright, "How the Comodo Certificate Fraud Calls CA Trust into Question," *Arstechnica*, 24 March 2011, http://arstechnica.com/security/2011/03/how-the-comodo-certificate-fraud-calls-ca-trust-into-question/1/ (accessed 24 October 2012); Peter Bright, "Independent Iranian Hacker Claims Responsibility for Comodo Hack," *Wired*, 28 March 2011, http://www.wired.com/threatlevel/2011/03/comodo_hack/ (accessed 24 October 2012).

[4] Gregg Keizer, "Firm Points Finger at Iran for SSL Certificate Theft," *Computer World*, 23 March 2011, https://www.computerworld.com/s/article/9214998/Firm_points_finger_at_Iran_for_SSL_certificate_theft? (accessed 24 October 2012).

[5] "Rogue SSL Certificates ('Case Comodogate')," *F-secure*, 23 March 2011, http://www.f-secure.com/weblog/archives/00002128.html (accessed 24 October 2012).

[6] "Iranian Anti-censorship Software 'Simurgh' Circulated with Malicious Backdoor (Updated)." *Citizen Lab*, 25 May 2012, https://citizenlab.org/2012/05/iranian-anti-censorship-software-simurgh-circulated-with-malicious-backdoor-2/ (accessed 24 October 2012).

and German powerhouse Siemens, is suspected of selling a sophisticated electronic surveillance system capable of monitoring Internet use. According to *The Washington Times*, "a spokesman for NSN said the servers were sold for 'lawful intercept functionality,' a technical term used in the mobile phone industry to refer to law enforcement's ability to tap phones, read e-mails, and survey electronic data on communications networks."[7] In June 2010, NSN acknowledged that it had sold equipment capable of tapping phone calls to the Iranian Telecommunications Company, but has denied that it provided Iran with software designed to intercept data and monitor Internet usage.[8] In August 2010, Isa Sarakhiz, an Iranian journalist and dissident, sued NSN, accusing the company of supplying the Iranian regime with spying technology.[9]

Similarly, a group of Western technology companies—Ericsson AB, Creativity Software Ltd., and AdaptiveMobile Security Ltd.—have been accused of marketing or providing equipment to Iranian law-enforcement and security agencies since 2009.[10] Of particular note are location-monitoring systems sold by Ericsson and Creativity Software, which Iranian authorities used to monitor political activists before apprehending and interrogating them. Ericsson has confirmed that it sold such technology to Iran, though it claimed that it distributed the technology to a mobile provider for customer-billing purposes. In late 2009, the company supplied Irancell, the country's second-largest mobile provider, with its Mobile Positioning System 9.0, which tracks and logs a mobile user's geographic position. Creativity Software and AdaptiveMobile have similarly admitted to providing services inside Iran, although they have declined to comment on the subject of government clients. AdaptiveMobile entered into an agreement with the government-controlled Mobile Communication Company of Iran to supply technology capable of intercepting text messages at a rate of 10,000 messages per second and storing them for 180 days. Creativity Software, for its part, reportedly sold customer-location services and law-enforcement tracking systems in 2010.

Supplementing purely technical tactics, the Iranian government has used the Internet to engage in simpler forms of surveillance. During the Green Movement demonstrations, the IRGC posted candid photos of protestors on its *Gerdab.ir* website and asked citizens to call or e-mail in their identities.[11] The post resulted in the arrest of at least two dissidents, but supporters of the protest movement responded with an image identification campaign of their own, aimed at exposing Iranian security forces and undercover agents.[12]

[7] Eli Lake, "Fed Contractor, Cell Phone Maker Sold Spy System to Iran," *The Washington Times*, 13 April 2009, http://www.washingtontimes.com/news/2009/apr/13/europe39s-telecoms-aid-with-spy-tech/print/ (accessed 24 October 2012).

[8] Tom Espiner, "Nokia Siemens Denies Iran Web Snoop," *ZDNet*, 22 June 2009, http://www.zdnet.com/nokia-siemens-denies-iran-web-snoop-4010013007/ (accessed 24 October 2012).

[9] "Activist Sues Nokia Siemens in US Over Iran Cell Monitoring," *Agence France-Presse*, 17 August 2010, http://www.google.com/hostednews/afp/article/ALeqM5iqerJYpKhH6VykIreWspndDE0jmA (accessed 24 October 2012).

[10] Ben Elgin, Vernon Silver, and Alan Katz, "Iranian Police Seizing Dissidents Get Aid of Western Companies," *Bloomberg*, 30 October 2011, http://www.bloomberg.com/news/2011-10-31/iranian-police-seizing-dissidents-get-aid-of-western-companies.html (accessed 24 October 2012).

[11] "Identify Rioters (First List)," [in Farsi] *Gerdab.ir*, 21 June 2009, http://www.gerdab.ir/fa/pages/?cid=407 (accessed 25 October 2012).

[12] Fred Petrossian, "Iranian Officials 'Crowd-source' Protester Identities," *Global Voices*, 27 June 2009, http://globalvoicesonline.org/2009/06/27/iranian-officials-crowd-source-protester-identities-online/ (accessed 24 October 2012).

End of Box 2

IRANIAN CYBER ARMY

While the National Information Network represents an attempt to shape cyberspace according to Iranian values by creating an isolated "cyberzone," the government has also aggressively promoted those values on the World Wide Web. "Internet brigades"—both official and unofficial—have waged online campaigns that promote a national narrative and combat competing ideologies.

Hacking collectives have been active in Iran since the early 2000s. Groups like Ashiyaneh, Shabgard, and Simorgh infiltrated government websites for the sake of notoriety, competition, and occasionally profit.[92] Beginning in the summer of 2009, politically motivated attacks and website defacements became increasingly common in Iran.[93] One group in particular, the self-described Iranian Cyber Army (ICA), has waged a concentrated effort to promote the Iranian government's political narrative online. ICA hackers have successfully defaced sites like Twitter, Voice of America, Baidu, and Radio Zamaneh, often emblazoning pages with their logo and leaving pro-government messages. Through such activities, the ICA seeks to induce fear, foment chaos, and hinder any web-based mobilization on the part of the opposition.

There is little concrete information about the ICA's origins, affiliations, or power structure. There have been reports of tenuous links between the ICA and the IRGC, with some claims that the ICA is a direct offshoot of the IRGC.[94] Ambiguous statements by Iranian officials have further obscured the ICA's nature. In 2010, the leader of the IRGC's Ali Ebn-e Abitaleb corps in Qom, Ebrahim Jabbari, openly claimed that his organization possessed the world's second-largest cyber army.[95] Although another IRGC official, Brigadier General Gholamreza Jalali, did not acknowledge any formal links between the two organizations, in 2011 he stated that "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."[96] In February 2012, Jalali also publicly stressed the importance of Iran building a "cyber army."[97] Whether or not the "cyber army" in these statements refers to the ICA is unclear. Other government sources have completely denied that the ICA holds any official status. In an interview with *Hamshahri Daily*, the director of Gerdab specifically clarified that his organization is not "after hacking and infiltrating like the Cyber Army" and described the ICA as simply a grassroots organization of cyber

[92] Farvartish Rezvaniyeh, "Pulling the Strings of the Net: Iran's Cyber Army," PBS, 26 February 2010, http://www.pbs.org/wgbh/pages/frontline/tehranbureau/2010/02/pulling-the-strings-of-the-net-irans-cyber-army.html (accessed 24 October 2012); Khashayar Nouri, "Cyber Wars in Iran," *Institute for War and Peace Reporting*, 23 July 2010, http://iwpr.net/report-news/cyber-wars-iran (accessed 24 October 2012).

[93] Amir Bagherpour and Roya Soleimania, "Oppression 2.0: Iranian Discontent in Cyberspace," *PBS*, 22 July 2011, http://www.pbs.org/wgbh/pages/frontline/tehranbureau/2011/07/oppression-20-iranian-discontent-in-cyberspace.html (accessed 24 October 2012).

[94] "Iran Cyber Army Hacks Former President's Websites," *Payvand Iran News*, 28 February 2012, http://www.payvand.com/news/12/feb/1282.html (accessed 24 October 2012).

[95] Rezvanieyeh, "Pulling the Strings of the Net."

[96] Golnaz Esfandiari, "Iran Says It Welcomes Hackers Who Work for Islamic Republic," *Payvand Iran News*, 7 March 2011, http://www.payvand.com/news/11/mar/1062.html (accessed 24 October 2012).

[97] "'Iran Set to Build First Cyber Army," *PressTV*, 20 February 2012. http://www.presstv.ir/detail/227739.html (accessed 24 October 2012).

activists.[98] Thus, the relationship between the government and the ICA is largely ambiguous. As in other cases, it is difficult to distinguish between nongovernmental collectives that the government tacitly supports and those that it directly or indirectly creates.[99]

There is likewise little information on the identities of those involved with the ICA's activities. Its numbers have purportedly reached 120,000.[100] The group's online presence is somewhat mysterious; it has presented the public with three different e-mail addresses that have appeared in messages posted on the websites that the Cyber Army had attacked.[101] The ICA also has no official website. Two of the e-mails that the Cyber Army has posted as part of its messages were created on private domains: soldier[at]cyberarmyofiran[dot]com and soldier[at]ircarmy[dot]com. Both domain names are currently dead. Our research indicates that a blog related to the ICA exists, listed as ircarmy[dot]persianblog[dot]ir. This blog is registered under persianblog[dot]ir, a Farsi blog platform. However, according to the blog's title, it is affiliated with the Cyber Army outside of Iran.

[98] "Conversation with the Administrator of Gerdab Website About Surveillance of Sites," [in Farsi] *Hamshahari Magazine Groups*, 22 October 2010, http://www.hamshahrimags.com/NSite/FullStory/News/?Id=4704 (accessed 30 March 2012).

[99] "Investigating the Activities of Syrian Cyber Army," [in Farsi] *Teribon*, 6 June 2011, http://www.teribon.ir/archives/54612 (accessed 24 March 2012).

[100] Fassihi, "Iran's Censors Tighten Grip."

[101] Iranian[dot]cyber[dot]army[at]gmail[dot]com, was the first e-mail made public through defacement messages, such as those posted on Twitter on 18 December 2009; soldier[at]cyberarmyofiran[dot]com appeared as the contact information for the ICA in the message left on the Chinese search engine Baidu, on 12 January 2010; soldier[at]ircarmy[dot]com, was the third e-mail address provided to date, and listed as an "alternative e-mail" on the message targeting Baidu.

BOX 3: CYBER ARMY ATTACKS

Starting from late 2009, the ICA has carried out numerous attacks against both Iranian and non-Iranian websites. These websites include (in chronological order from December 2009 to date): Green Wave of Freedom,[1] Twitter,[2] Baidu,[3] Radio Zamaneh,[4] Amir Kabir Newsletter,[5] The Official Website of Mohsen Sazegara,[6] Jaras,[7] Tech-Crunch,[8] Farsi Television One and other Moby Group Websites,[9] Voice of America (VOA),[10] and AZ-TV (Azerbaijan's State TV).[11] The messages left by the ICA-affiliated attackers on their targets' websites indicate that the group's motives are based on ideology and nationalistic aspirations. Upon hacking Twitter, for example, the ICA left the following poem dedicated to Ayatollah Khamenei:

> If the Leader orders, we will rush forward
> If he asks us, we will offer our heads
> If he wants us to be patient, we will tolerate and bear it.[12]

Similar messages were posted on opposition and dissident websites. A different tactic was employed against TechCrunch, a technology and Internet blog. The ICA hacked the website and thereafter directed users to a corrupt server that collected their information and attempted to install malware on their computers.[13]

[1] "Moje Sabz Website Has Been Hacked," [in Farsi] *Khabar Online*, 16 December 2009, http://www.khabaronline.ir/news-30712.aspx (accessed 20 March 2012).

[2] Robert Mackey, "Twitter Attacked by 'Iranian Cyber Army,'" *New York Times*, 18 December 2009, http://thelede.blogs.nytimes.com/2009/12/18/twitter-hacked-by-iranian-cyber-army/ (accessed 20 March 2012).

[3] "Chinese Website Attacked by 'Iranian Cyber Army,'" [in Farsi] *BBC Persian*, 12 January 2010, http://www.bbc.co.uk/persian/science/2010/01/100112_l02_china_internet_iran.shtml (accessed 22 March 2012).

[4] "Radio Zamaneh's Website Has Been Hacked," [in Farsi] *Fars News Agency*, 31 January 2010, http://www.farsnews.com/newstext.php?nn=8811110874 (accessed 22 March 2012).

[5] Saleh Ruhollah, "Everything About Iranian Cyber Army," [in Farsi] *Azarbad*, 18 February 2010, http://saleh.ruhollah.org/368 (accessed 24 March 2012).

[6] "Sazegara's Website Has been Hacked," [in Farsi] *Tabnak News*, 17 February 2010, http://www.tabnak.ir/fa/news/85501/%D8%B3%D8%A7%D9%8A%D8%AA-%E2%80%8C%D8%B3%D8%A7%D8%B2%DA%AF%D8%A7%D8%B1%D8%A7-%D9%87%D9%83-%D8%B4%D8%AF-+%D8%B9%DA%A9%D8%B3 (accessed 24 March 2012).

[7] "New Cyber Attacks Hit Iranian Opposition Websites," [in Farsi] *BBC Persian*, 12 February 2010, http://www.bbc.co.uk/persian/iran/2010/02/100212_l06_jaras_kalameh_hacking.shtml (accessed 24 March 2012).

[8] "The 'Iranian Cyber Army' Strikes Back," *Seculert Blog*, 24 October 2010, http://blog.seculert.com/2010/10/iranian-cyber-army-strikes-back.html (accessed 24 March 2012).

[9] Iran Cyber Army, "Happy *Eid al-Adha*," November 2010, http://sarzaminebalatarin.files.wordpress.com/2010/11/ghorban05.jpg (accessed 24 March 2012).

[10] "Voice of American and Ninety-five Affiliated Websites Were Hacked by Iranian Cyber Army," [in Farsi] *Fars News Agency*, 2 June 2010, http://www.farsnews.com/newstext.php?nn=8912030160(accessed 22 March 2012).

[11] "Iran Cyber Army Hits Azerbaijan State TV Site," [in Farsi] *BBC Persian*, 23 February 2012, http://www.bbc.co.uk/persian/iran/2012/02/120223_008-iran-azerbaijan.shtml (accessed 26 February 2012).

[12] Scott Peterson, "Twitter Hacked: 'Iranian Cyber Army Signs off with Poem to Khamenei," *The Christian Science Monitor*, 18 December 2009, http://www.csmonitor.com/World/Middle-East/2009/1218/Twitter-hacked-Iranian-Cyber-Army-signs-off-with-poem-to-Khamenei (accessed 24 October 2012).

[13] Jeremy Kirk, "Iranian Cyber Army Running Botnets, Researchers Say," *Computer World*, 25 October 2010, https://www.computerworld.com/s/article/9192800/Iranian_Cyber_Army_running_botnets_researchers_say (accessed 24 October 2012).

BOX 4: IRANIAN MEDIA CENSORSHIP AND THE ARAB SPRING

In addition to the Internet and new media, the Iranian regime has applied its policy of altering information flows to fit an official political narrative to traditional forms of media. In August 2012, Egyptian president Mohammed Morsi gave a speech in Iran during the Nonaligned Movement (NAM) summit. However, what the Iranian audience heard was a very different interpretation of President Morsi's message thanks to the Arabic-Farsi translators on state-affiliated television and radio stations. The interpreter changed the wording so that the Farsi version of the speech appeared more aligned with the Iranian government's policy towards Syria, Bahrain, and the Arab Spring.

President Morsi's repeated references to Syria and the people's struggle there were consistently changed to "Bahrain" in the Farsi translation. A mention of "oppression and repression" referring to the Syrian government was dropped in favour of an alleged "conspiracy against the country." In perhaps the most blatant example, his statement that "unity of the Syrian opposition is necessary" was reproduced as "we hope that the regime, which enjoys popular support, will continue to be there." The term Arab Spring was also changed to "Islamic Awakening."[1]

This form of distorting censorship highlights a number of issues. First, the Iranian regime seeks to filter out information that contradicts its formal policy on political issues such as the Syrian conflict. Iran has supported the Syrian regime against the popular uprising, but has also spoken out against the Bahraini government over its attempt to combat popular demands for democratic change. Second, the Iranian regime and affiliated media outlets have consistently labelled the uprisings and revolutions across the Middle East and North Africa since 2011 an "Islamic Awakening" instead of the more popular term: "Arab Spring." This represents the regime's clear attempt to portray the democratic demonstrations as if they were aligned with the Islamic Revolution of 1979. Third, this example highlights the difficulty of reversing the impact of censorship— Iranian citizenry are unlikely to have access to the correctly translated version of the speech. All told, this example of media manipulation is consistent with the regime's broader censorship policy that attempts to systematically control flows of information.

[1] "Al-Jazeera Report on Iranian Television's Misrepresentation of Morsi's Speech," 1 September 2012, http://www.youtube.com/watch?v=SWhfIEW1Smw (accessed 25 October 2012).

end of Box 4

GEO-POLITICS

Control of information in Iran is not simply a matter of domestic stability. The regime views cyberspace as a battleground upon which conflicts are fought with foreign powers by means of "hard" and "soft" power. Hard power refers to typical elements of cyberwarfare—malware, viruses, trojans —which Iran has been a target of since at least 2010. In June 2010, a Belarusian antivirus company discovered a computer worm named Stuxnet.[102] The virus had accidentally spread beyond its target, Iran's uranium enrichment facilities at Natanz, where it was intended to disrupt or destroy centrifuge control systems. According to a number of sources, Stuxnet did a significant amount of damage to Iran's nuclear enrichment program. Centrifuge capacity at the plant allegedly dropped by 30 percent between 2009 and 2010[103] and up to 1,000 centrifuges may have been destroyed as a direct result of the virus.[104] A related worm, called Duqu, was discovered by CrySys Lab at Budapest University of Technology and Economics in September 2011. Duqu is supposed to be very similar to Stuxnet, but functions by exfiltrating data about industrial control systems rather than destroying them outright. Most recently, a consortium of researchers announced the discovery of a cyber-espionage malware named Flame in May 2012. Flame is capable of recording audio, video, keyboard strokes, screenshots, and network traffic, among other functions, and relaying that information to central command-and-control servers scattered around the globe. All three programs, and possibly others still undiscovered, are suspected components of "Operation Olympic Games," a series of attacks allegedly launched collaboratively by the United States and Israel against Iranian nuclear facilities.[105] The Iranian government's continued emphasis on the importance of developing an isolated intranet as a defence mechanism against foreign aggression and its insistence on central control through bodies like the Supreme Council on Cyberspace must be understood in this context.

However, beyond blatant attacks, Iran has also made reference to the West's exercise of "soft" power that is meant to undermine the country's political stability, Perso-Islamic culture, and societal unity. Western displays of soft power often adopt the rhetoric of freedom, openness, and

[102] Gregg Keizer, "Is Stuxnet the 'best' malware ever?" *InfoWorld*, 16 September 2010, http://www.infoworld.com/print/137598 (accessed 20 November 2012).

[103] Yossi Melman, "Computer Virus in Iran Actually Targeted Larger Nuclear Facility," *Haaretz*, 28 September 2010, http://www.haaretz.com/print-edition/news/computer-virus-in-iran-actually-targeted-larger-nuclear-facility-1.316052 (accessed 24 October 2012).

[104] David Albright, Paul Brannan, and Christina Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?" Institute for Science and International Security, 1 http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/ (accessed 25 October 2012).

[105] David Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, 1 June 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0 (accessed 20 November 2012.

democratic accountability. For example, in 2010, US Secretary of State Hilary Clinton explicitly referred to Iran in her speech on Internet freedom. With reference to the 2009 election protests, she said:

> As in the dictatorships of the past, governments are targeting independent thinkers who use these tools. In the demonstrations that followed Iran's presidential elections, grainy cell phone footage of a young woman's bloody murder provided a digital indictment of the government's brutality. We've seen reports that when Iranians living overseas posted online criticism of their nation's leaders, their family members in Iran were singled out for retribution. And despite an intense campaign of government intimidation, brave citizen journalists in Iran continue using technology to show the world and their fellow citizens what is happening inside their country. In speaking out on behalf of their own human rights, the Iranian people have inspired the world. And their courage is redefining how technology is used to spread truth and expose injustice.[106]

Secretary Clinton's open declaration of "Congress's and the American people's commitment to Internet freedom, a commitment that crosses party lines and branches of government"[107] in the same speech indicates that the US sees the promotion of Internet freedom as one of its many foreign policy commitments. It is clear that US policymakers view Iran as a highly repressive country and thus a key target for promoting Internet freedom.

Wary of the Internet's role in anti-government activity and equally concerned about Western influence in Iran, the Iranian government believes itself engaged in a "soft war" launched by foreign powers against the Islamic government.[108] As Babak Rahimi writes, "when the [Internet] began to be increasingly used by Iranian dissidents, post-election cyberactivism came to be viewed as a type of cyberwarfare led by foreign agents, namely Britain and the United States."[109] The regime interprets the US government's commitment to an open cyberspace as nothing more than a pretext for propaganda aimed at Westernizing Iran. The fear of foreign influences corrupting Iran's Perso-Islamic culture has precedents. In the 1960s, Jalal Al-e Ahmad popularized the term "Westoxification" (*Gharbzadegi*) in a book published under the same name. For Al-e Ahmad, *gharbzadegi* is a worldwide epidemic, in which the industrialized rich world of the West aggressively exports its culture to the East, Iran included.[110] Moreover, the "West thrusts its 'machines' upon Iran in order to frighten, exploit, and control Iranians."[111] In response, Iran and the East may adopt one of three courses: submit to the West's machines; retreat into traditional cultures; or, most preferably, tame the "machine" and make it Iranian. Years later 'Ali Shari'ati drew heavily upon Al-e Ahmad's philosophy of anti-Westernization to formulate the Islamic ideology that informed Ayatollah Khomeini and underpinned the 1979 revolution.

Today, the idea of a cultural assault from the

[106] Hillary Clinton,US Department of State, "Remarks on Internet Freedom," Last modified 2010, http://www.state.gov/secretary/rm/2010/01/135519.htm (accessed 25 October 2012)..

[107] Ibid.

[108] Robert F. Worth, "Iran Expanding Effort to Stifle the Opposition," *New York Times*, 23 November 2009, http://www.nytimes.com/2009/11/24/world/middleeast/24iran.html?_r=2&ref=world (accessed 25 October 2012).

[109] Rahimi, "Agnostic Social Media," 170.

[110] Brad Hanson, "The Westoxification of Iran: Depictions and Reactions of Behrangi, al-e Ahmad, and Shariati," *International Journal of Middle East Studies* 15, no. 1 (February 1983): 10.

[111] Ibid., 11.

West still informs the Iranian regime's rhetoric and provides ample justification for filtering, censorship, and surveillance. Days after Ms. Clinton's second speech on Internet freedom, the websites of Voice of America's (VOA) Persian service were attacked by the Iranian Cyber Army. The defacement message proclaimed: "We have proven that we can. Mrs. Clinton, do you want to hear the voice of oppressed nations will from heart of USA? Islamic world doesn't believe USA trickery. We call on you to stop interfering in Islamic countries."[112] This defacement speaks of the US as a threat—the attack itself came after a speech by the Supreme Leader Ayatollah Khamenei calling on "Muslim nations and government to become vigilant and stop the 'great Satan' (the US) from interfering in their destinies."[113] Iran simultaneously accuses Western governments of hypocrisy regarding Internet filtering on its *Peyvandha* website. A page titled "Internet Monitoring in Other Countries" gives a summary of online content being filtered and monitored in different countries including the United States, China, Europe, and the Middle East. The page places particular emphasis on Gmail's affiliation with the American government, and its utility as a spying tool.

This "soft" geopolitical war has justified steps towards Iran's National Information Network and an organized, security-conscious approach toward cyberspace. The creation of the Supreme Council on Cyberspace denotes the significance of ICTs to the Supreme Leader as a field that requires direct involvement and intervention. It elevates the status of cyberspace to an arena of foreign policy and national security, and highlights the struggle that the Iranian government has faced since at least 2009. The need to strike a balance between the economic and political advantages the Internet confers and the previously unprecedented dangers that it brings to the regime has been evident in the state's rhetoric. Ayatollah Khamenei has referred to the Internet as a "double-edged knife" and as an "ever-flowing and violent river" – one that can deliver opportunities when controlled and guided, but that poses a threat when left to itself.[114] The Internet has been specifically singled out as a weapon of war against the country. Authorities have repeatedly indicated the post-presidential election unrest in 2009 as one of the most tangible instances of such a war.[115] The Social and Cultural Deputy of the IRGC has claimed that, "today, the weapons of war are not tanks, bombs and missiles" – rather, warfare against the Islamic Republic takes place in the field of cyberspace, Internet, and satellite TV.[116] Operations like Stuxnet have also precipitated strong arguments against the Internet and "fed into this sense that Western services are agents in a soft war."[117]

[112] "The Iranian Cyber Army's Attack on Voice of America's Website," [in Farsi] 21 February 2011, http://www.voanews.com/persian/news/voa-cyberattack-2011-02-21-116608413.html (accessed 25 October 2012).

[113] "Supreme Leader Warns of Hegemonic Powers' Plots Against Muslim Unity," *Fars News Agency*, 2 February 2011, http://english.farsnews.com/newstext.php?nn=8912020581(accessed 25 October 2012).

[114] "What Are the Missions of the Supreme Council on Cyberspace?" [in Farsi] *Fars News Agency*, http://www.farsnews.com/newstext.php?nn=13901226000466 16 March 2012 (accessed 4 April 2012).

[115] The Internet One of the Tools of the 2009 Sedition," [in Farsi] *Mag-Iran*, 28 February 2011, http://www.magiran.com/npview.asp?ID=2248181 (accessed 4 April 2012).

[116] "Why and for What Reason Was the Supreme Council on Cyberspace Created?" [in Farsi] *Jahan News*, 17 March 2012, http://jahannews.com/vdcb8fb5grhb8zp.uiur.html (accessed 3 April 2012).

[117] Riesman, "Iran's Network."

Fear of foreign cultural influence in the media and cyberspace, however, has not meant that Iran has remained completely isolated in a sort of technological autarky. As outlined earlier, Iran has contracted European companies to provide the regime with surveillance equipment. More recently, Iran has seen partnerships with non-Western companies, such as the China-based telecommunications giant Huawei Technologies Company, as a solid alternative to reliance on Western corporations. Huawei itself has publicly dismissed as baseless various allegations that it violated international sanctions against Iran.[118] However, the *Wall Street Journal* sees reports that mobile technology supported by Huawei was also used to arrest dissidents as the primary motivation for the company to scale back business with Iran.[119] Huawei's announcement that it would "voluntarily restrict its business development [in Iran] by no longer seeking new customers and limiting its business activities with existing customers" in light of the "complex situation" in the country also came with an assurance that their business operations in Iran were conducted in "full compliance with all applicable laws and regulations including those of the UN, US and EU."[120] Months after Huawei opted to scale back their Iranian operations, reports showed that ZTE Corp, another Chinese telecom, sold TCI a powerful surveillance system capable of monitoring Internet communications as well as messages over mobile and landline networks.[121]

Much of Iran's telecommunications infrastructure is dependent on international links and agreements with Russia and Central Asian countries. Iran's international Internet connections are through the UAE, Turkey, and recently, via Azerbaijan to Russia. Renesys has described Iran's purchase of Russian transit as part of a "geopolitical diversity" strategy and one facet in a larger context of a new strengthening in Iranian-Russian relations, including coordination in the military and energy domains.[122] Relations with Russia can also be seen in light of Iran's involvement in the Shanghai Cooperation Organization (SCO) as an observer state. The SCO, comprised of Russia, China, Kazakhstan, Tajikistan, Kyrgyzstan, and Uzbekistan, was originally created as a multilateral vehicle to ensure security coordination between member states, its focus being on "terrorism, separatism, and extremism."[123] "Subversion" through the Internet has long been a theme running through the SCO's rhetoric on cyberspace. In 2009, the SCO approved an agreement that Russia proposed to define "information war" as one state's way to undermine another state's political, economic, or social system.[124] This agreement also stated that

[118] Steve Stecklow, "Lawmakers Ask State Department to Probe Huawei Business with Iran," *The Wall Street Journal*, 5 January 2012, http://online.wsj.com/article/SB10001424052970203513604577140700603637204.html (accessed 25 October, 2012).

[119] Worth, "Iran Expanding Effort."

[120] Huawei, "Statement Regarding Huawei's Commercial Operations in Iran," http://www.huawei.com/en/about-huawei/newsroom/press-release/hw-104866-statement-commercialoperations.htm (accessed 25 October 2012).

[121] Steve Stecklow, "Special Report: Chinese Firm Helps Iran Spy on Citizens," *Reuters*, 22 March 2012, http://www.reuters.com/article/2012/03/22/us-iran-telecoms-idUSBRE82L0B820120322 (accessed 25 October 2012).

[122] James Crowie, "The Geopolitics of Iranian Connectivity," *Renesys Blog*, 11 February 2010, http://www.renesys.com/blog/2010/02/irans-internet-the-geopolitics.shtml (accessed 25 October 2012).

[123] Julie Boland Brookings, "Ten Years of the Shanghai Cooperation Organization: A Lost Decade? A Partner for the US?" http://www.brookings.edu/~/media/research/files/papers/2011/6/shanghai cooperation organization boland/06_shanghai_cooperation_organization_boland (accessed 25 October 2012), 5.

[124] Ibid., 13.

information “harmful to the spiritual, moral and cultural spheres of other states” should be seen as “security threat.”[125] While there is little evidence of the SCO being a vehicle for member states to exchange knowledge, expertise, and technology related to filtering and information controls, it seems likely that part of Iran’s geopolitical attraction to the organization is an ostensible similarity in vision, values, and attitudes towards the Internet. The SCO’s language to describe information warfare as fundamentally a war of ideas, culture, and social harmony is remarkably similar to public statements made by various Iranian religious, political, and military leaders.

[125] Tom Gjelten, “Seeing the Internet as an ‘Information Weapon,’” NPR, http://www.npr.org/templates/story/story.php?storyId=130052701 (accessed 25 October 2012).

CONCLUSION

It remains unknown whether the information-control mechanisms created by the Iranian government have effectively prevented anti-regime activity. The Iranian blogosphere has been noted for its size and diversity of voices and is highly active despite extensive filtering.[126] Circumvention of Internet filters through proxies and VPNs is commonplace.[127] However, the existence of passive resistance online has not necessarily translated into a successful revolutionary movement. As the Green Movement was organizing protests in 2009, Palfrey, Elfrey, and Faris argued that social media sites such as Twitter have severe limits as far as engendering political activism due to character limits and the constant noise of incoming "tweets" drowning out relevant messages.[128] Investigations have shown that the social media "footprint" of dissidents and anti-regime activists *outside* of Iran has been used by the government to track and persecute them.[129]

It is difficult to say whether the subsequent movement towards greater second- and third- generation controls has also stifled the opposition's presence in cyberspace. Certainly laws against VPN use and the passing of the Cyber Crimes Law have not prevented anti-filtration methods from being disseminated by ordinary Iranian citizens, nor have they eliminated dissident voices within the country or in the diaspora. But, in combination with more sophisticated monitoring techniques, they have raised the stakes for both users and providers, perhaps significantly enough to deter such activity. Likewise, the Iranian regime's ongoing attempts to "colonize" cyberspace through offensive (e.g., ICA propaganda campaigns) and defensive manoeuvres (e.g., the National Information Network) cannot totally prevent savvy citizens from accessing outside information. However, closing the boundaries and dominating the airwaves of informational space will limit the consumption and dissemination of opposing viewpoints.

The next twelve months are likely to be eventful for Iran. The first presidential election since that which spawned the Green Movement will be held in June 2013 and the regime will undoubtedly be on the lookout for any sign of unrest or protest as citizens go to the ballot boxes. Monitoring and

[126] John Kelly, and Bruce Etling, "Mapping Iran's Online Public: Politics and Culture in the Persian Blogosphere," Berkman Center for Internet and Society at Harvard University, Internet and Democracy Case Study Series, 1-36, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Kelly&Etling_Mapping_Irans_Online_Public_2008.pdf (accessed 16 October 2012), 5.

[127] Freedom House, "Iran: Freedom on the Net 2012," last modified 2012, http://www.freedomhouse.org/report/freedom-net/2012/iran (accessed 16 October 2012).

[128] John Palfrey, Etling Bruce, and Faris Robert, "Why Twitter Won't Bring Revolution to Iran," *The Washington Post*, 21 June 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/06/19/AR2009061901598.html (accessed 25 October 2012).

[129] Farnaz Fassihi, "Iranian Crackdown Goes Global," *The Wall Street Journal*, 3 December 2009, http://online.wsj.com/article/SB125978649644673331.html (accessed 25 October 2012).

filtering of blogs and social network sites will likely intensify beyond already high levels. State-sponsored targeted malware attacks—of which very few have been reported in Iran since 2009—may appear as a means of dissuading dissidents or keeping tabs on unaware opponents. Targeted malware directed toward opposition activists have been especially prevalent in the context of Syria's ongoing civil conflict.[130] It is possible that the Iranian government or the ICA will employ similar programs if the Internet once again becomes a forum for popular organization. The Iranian government may also try to launch a version of its National Information Network prior to the elections, thereby controlling information flows on Iran's intranet and facilitating surveillance of those who remain on the Internet. It is likely that all of these initiatives will come under the guise of "national security" to some extent as Western states continue to impose sanctions, initiate cyber attacks, and encourage civil society to take action.

One can argue that the Iranian government has undergone a learning period since 2009. With the use of ICTs by both pro- and anti-regime forces in many of the contemporary "Arab Spring" revolutions, it is not difficult to imagine the Iranian government taking heed of recent regional developments to move towards a fortress-style model of cyberspace. With this analysis in mind, utopian models of cyberspace as an inevitable harbinger of greater openness must take into account the possibilities that states can adapt technology to counter democratic freedoms in much the same way that citizens adapt technology to fight for them.

[130] "Syrian Activists Targeted with BlackShades Software," Citizen Lab, 19 June 2012, https://citizenlab.org/2012/06/syrian-activists-targeted-with-blackshades-spy-software/ (accessed November 27, 2012).