AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

IRANIAN NATIONAL INFORMATION NETWORK

By

Sean A. Williams, Maj, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements for the Degree of

MASTER OF OPERATIONAL ARTS AND SCIENCES

Advisor: Dr. Johnathan K. Zartman

Maxwell Air Force Base, Alabama

December 2019

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Abstract

Iranian protests in the new millennium have depended on the Internet for organization and communication. Additionally, exiled Iranians have used the Internet to distribute material to both worldwide audiences and the internal population of Iran. The Iranian government views digital communications and the Internet as powerful tools, but is also aware of the danger they pose to their authority. The Iranian government has undertaken a massive project named the National Information Network (NIN) to provide better connectivity to their populace and to better control communication--both inside and leaving Iran. This paper will discuss the history of telecommunications in Iranian protests, common techniques for censorship of the Internet, previous government attempts at controlling communications, a background on the NIN, and its capabilities to block protestor communications. Finally, it conclude that the NIN will make dissident communications more difficult, but will ultimately be unable to effectively stop protest organinizing due to workarounds.

Background on Telecommunications in Iranian Protests

Technology has long had a significant role in organizing protests: protest organizers actively employed technology to mobilize supporters to demonstrate in the 2009 Green Movement. The use of social media, in particular, was so prevalent that the protests became known as the "Twitter Revolution." Protestors used services such as Facebook, Twitter, blogs, email, online newsletters, and short message service (SMS) to organize and discuss strategies for their demonstrations. Technology companies assisted by adding Persian versions of their websites. Protestors also used these sites to document atrocities by posting mobile phone recordings of such acts as the beatings of women and children. Exiled spiritual leaders contributed to the discussions due to the increased global integration of technology in Iranian life.[1]

Eight years later in Dec 2017, Iranians across the country protested the state's bad economy and failures of the reformist government. An application named Telegram proved critical for organizing and discussing the movement. Of the 80 million people in Iran, estimates show that 40 million people used the free application that allows encrypted sharing of messages, videos, and photos. For example, Roohallah Zam, an exiled journalist and activist, used Telegram to coordinate protests and share videos from demonstrations.[2] Despite a government block of Telegram, many Iranian users continued to access the service through anonymization services such as Tor (also previously known as The Onion Routing) or using encrypted communications to intermediary systems outside Iran called virtual private network (VPN) providers.

In addition to using Telegram, Iranian exiles utilized social media sites such as Facebook to organize activist events. Examples of two prominent social media campaigns were "My

Stealthy Freedom" and "White Wednesdays." Since 2014, exiled Iranian journalist and activist Masih Alinejad has led the "My Stealthy Freedom" movement to protest state compulsion on women to wear a hijab in Iran, she collected and posted images of women in public without hijabs. She used social media "as a weapon" to promote change.[3] In late 2017, in conjunction with that protest, Alinejad started the "White Wednesdays" campaign, in which women in Iran were removing their hijabs and waving them on a stick. Activists publicized these protests via social media and added women's issues to the 2017-2018 protests.[4]

A 200% increase in fuel prices in Nov 2019 led to protests in multiple cities across Iran that quickly turned into general anti-government protests. As of early December 2019, data on the role of digital communications in the spread of the protests remains unavailable. As the protests grew, the government of Iran nearly completely disconnected the country from the Internet, Oracle's Director of Internet Intelligence described this as "arguably the largest event ever for Iran."[5]

Methods of Internet Censorship

Before discussing how the government of Iran reacted to each of these events, this paper will provide a high-level explanation of government tactics to censor the Internet. Most states have multiple ISPs that provide connectivity to their population. Governments must coordinate censorship actions across these ISPs. The ISPs may utilize a variety of filtering and blocking techniques at various levels in network communications. Additionally, many of the techniques can be layered to more effectively prevent access to targeted resources. The section will describe each layer of the Transport Control Protocol/Internet Protocol (TCP/IP) stack (a model for typical Internet communication), some examples of common protocols in that layer, and the associated techniques used for censorship. Examples of each layer, protocols, aimpoints, and control measures can be found in Table 1.

Table 1. Targeting Options to for Government Censorship against Telecommunications Systems

TCP/IP Layer	Example Protocols	Aimpoints	Control Measures
Link	Wifi 802.11ac, Ethernet, Global System for Mobile Communications (GSM)	Device specific selectors	Block a specific device from a network (for government controlled networks)
Internet	Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6)	IP Addresses	Block IP addresses or blocks of IP addresses for blacklisted services
		Routing	Drop routes to blacklisted organizations
Transport	Transport Control Protocol (TCP) and User Datagram Protocols (UDP)	Ports	Block traffic for a service based on its standard ports
Application	Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS)	URLs	Filter based off keywords or domains in URLs
		Content	Filter based off keywords in content
	Transport Layer Security (TLS)	Certificates	Filter based off characteristics of certificate
	Domain Name Service (DNS)	Domain Queries	Drop or return bad data for blacklisted domains

The Link layer of the TCP/IP stack describes how two directly connected devices can communicate. Examples of Link layer protocols are Wifi 802.11ac, Ethernet, or Global System for Mobile Communications (GSM). Government controls will typically be at higher levels of the stack since Link layer controls would be too fine-grained for mass censorship.

The Internet layer specifies how two devices can communicate over inter-connected networks such as the Internet. The predominant standard for this layer, Internet Protocol (IP), designates standards for source and network IP addresses. Governments may implement blocks against specific IP addresses or blocks of IP addresses. Additionally, governments can manipulate the protocols that determine the routes for traffic to make, effectively denying communication on their networks to specific segments of the Internet.

The Transport layer allows traffic to facilitate connections, reliability, and multiplexing of communications. The primary Transport layer protocols are Transport Control Protocol (TCP) and User Datagram Protocol (UDP). TCP and UDP allow traffic to be associated with ports for a specific service. For example, the standard web traffic port is TCP port 80 and encrypted web traffic is TCP port 443. Governments can utilize the Transport layer to conduct more finely tuned blocks than those at the Internet layer (i.e., only block specific ports). Additionally, governments can stop all traffic associated with a service by blocking its standard port. A possible example of this would be to stop all encrypted web traffic by blocking TCP 443.

The Application layer defines how specific applications communicate with each other. Some common examples are Hypertext Transfer Protocol (HTTP) for web traffic, Transport Layer Security (TLS) for encrypted traffic, and Domain Name Service (DNS) for resolving domain names to IP addresses. Many of these Application layer protocols can be nested. For example, Hypertext Transfer Protocol Secure (HTTPS) utilizes the TLS protocol to encrypt HTTP traffic. Governments can utilize techniques that identify and block specific protocols such as HTTP or DNS. Additionally, governments may be able to manipulate the protocols to return manipulated results. An example is the interception of DNS requests for specific domains and replying with a false answer to either redirect or block communications. Furthermore, governments can utilize more advanced techniques known as Deep Packet Inspection (DPI) to inspect specific characteristics of traffic. An example is detecting and blocking specific cryptographic certificates associated with Instagram in TLS communications or filtering based on the information in the Uniform Resource Locator (URL) field of an HTTP request.

The Iranian government has utilized all of these techniques to censor communications, but often in seemingly haphazard ways. Although all international traffic ultimately flows through the state-owned Telecommunications Infrastructure Company (TIC), Iran's 11 different ISP companies have utilized different techniques in conjunction with the same events.[67] Additionally, the implementation of blocks across the ISPs sometimes occurred over multiple days (MCI blocking Telegram on 31 Dec 2017, Pars Online implementing the block on 1 Jan 2018, and Irancell implementing the block on 2 Jan 2018).[8] It is unclear why the blocks take place over multiple days, but it demonstrates differences in implementation with the various ISPs. All ISPs eventually implemented blocks, so it also shows compliance with censorship orders.[9]

Previous Government Attempts at Controlling Communications

The Iranian government has attempted to disrupt protestor communications in each of the previously discussed events. Over time, both protestor and government methods have become more sophisticated, but the government has taken increasingly drastic steps to disrupt communications. The next section will show this evolution by describing how the government responded to each of the protests.

The 2009 Green Movement actively used the Internet to spread protest messages. The government attempted to censor the communications by blocking communication to Facebook, Twitter, and other services. The government blocked IP traffic destined for these businesses, HTTP traffic with URLs matching these sites or other keywords, and ports associated with messaging or other services (such as Yahoo Messenger, or even all HTTPS for periods). It also occasionally throttled traffic speeds by randomly dropping packets to make technologies such as VPNs difficult to use.[10] Protestors were able to circumvent these controls through the use of proxies, virtual private networks (VPNs), and other censorship circumvention tools. The Iranian government attempted to block ports associated with VPN services, but the users were often quickly able to reestablish connections via other VPN ports.[11] The difficulty with effectively suppressing communications gained the attention of the government and led to increased efforts to develop technical and legal frameworks for censorship. The Iranian information controls progressed from restricting access to specific Internet resources via technical filtering to creating legalized controls and technical capabilities for "just-in-time" controls that deny access to specific information at key times. The aftermath of the 2009 Green Movement also resulted in the proposal for the development of a "Halal Internet" that would offer similar services to those used by protestors, but under complete government control. The government would attempt to motivate the populace to use these domestic services, while also restricting access to their non-Iranian counterparts.[12]

During the 2017-2018 protests, the government blocked popular applications across most of the Iranian Internet Service Providers (ISPs). About half of the Iranian ISPs blocked the TCP traffic for Telegram's web application and phone application.[13] Notably, all Instagram traffic was blocked using DPI techniques to detect and stop TLS traffic using Instagram's cryptographic certificate.[14] The ISPs had also previously censored Facebook Messenger by blocking DNS lookups associated with the service.[15] When blocks were implemented on these popular services, Iranian usage of the Tor anonymity network spiked for a few days before ISPs started making accessing the network more difficult. Circumvention of government censorship was still possible, however, via the use of VPN services, and configuring the Tor network to utilize alternative connection points called Tor bridges.[16]

During the recent 2019 protests the government employed the heaviest censorship of Internet usage to date. The government performed a nearly complete disconnection of the Iranian ISPs from the Internet starting on 15 Nov and lasting for multiple days.[17] Analysts have not documented the effectiveness of this blocking as of December 2019, but analysts reported that the level of disconnection severely hindered communication services. The disconnection affected not only the protestors, but also businesses and other government agencies from utilizing services on the Internet. For example, if any businesses had uploaded data to international cloud service providers, they could not access it during the disconnection, which has hurt businesses and services. Despite this, some individuals posted videos of the protests online during the outage, sometimes by traveling to borders and using other nations' ISPs.[18]

Background on the National Information Network (NIN)

In 2006, the government first proposed the National Information Network (NIN), a $6 billion Iranian government-controlled secure national network. A 2011-2016 Iranian government development plan defined the NIN as an "IP-based internet supported by data centers that are completely undetectable and impenetrable by foreign sources and allow the creation of private, secure intranet networks." The Stuxnet infections of 2010 further stimulated the creation of the NIN, which also sought to improve access to the Internet and move content and services to closely-monitored and censored domestic servers. The project has been actively developed in phases since its inception. The Information and Communication Technology (ICT) Ministry claims it has connected over 27,000 villages to high-speed Internet in the first four years of the Rouhani administration. Additionally, the ICT ministry stated that domestic traffic increased from 10% of all Iranian Internet usage to 40% from 2016 to March 2017. ISPs are further driving this trend by giving a 50% discount on bandwidth for domestic traffic.[19]

In order to further sever dependence on international resources, under another aspect of the NIN project, the government directed technology specialists to create domestic software and services such as data centers, web browsers, operating systems, search engines, social networks, e-mail, and even VPNs. Many of these discounted domestic programs provide services analogous to Twitter, Facebook, and Telegram, which strengthen the government's capability of control and surveillance to a level that most international businesses would never accept. Additionally, domestic software products such as web browsers have government-issued cryptographic certificates, which may allow authorities to inspect the browser's encrypted traffic.[20]

After each new service becomes ready, the government blocks access to the international site to drive traffic to the domestic service. However, traffic analysis shows that Iranian users had relatively little interest in the domestic alternatives when services such as Telegram were blocked. For example, when Telegram was blocked, the Tor anonymization project saw a sharp increase in usage, likely so that users could circumvent the blocks.[21]

Since the NIN developed slowly over the past decade, and analysts have yet to clearly document its architecture, observers cannot definitively assess the NIN's current capabilities. The NIN probably enabled many of the filtering capabilities and the recent isolation that the government used to suppress the 2018 and 2019 protests.[22] The groundwork for removing the dependence on critical international services seems complete, which should allow Iran to isolate itself from the Internet without catastrophic failures. An isolation such as this prevents even evasive anti-censorship communication methods such as VPNs and Tor from communicating out of traditional ISP routes.

Besides isolation, increases in intelligent monitoring and filtering have occurred over the development life of the NIN. In 2009, the government had to block whole sites. In 2014, Iranian filtering had progressed to the point of blocking individual pages based on content. For example, Iranian users could browse Wikipedia, but specific government-banned topics were inaccessible. This continued growth of monitoring and censorship capability has allowed Iran to be more suppress Internet freedom more than all other countries besides China.[23]

Also, the NIN project increased user attribution. The ICT deputy minister, Nasrollah Jahangard, stated that "all connections including mobile connections have identification; without identification, you will not be able to use the Network's services."[24] Additionally, the government requires ISPs to keep usage dates and times, allocated IP addresses, and logs of visited web pages for six months.[25] Iranians have long used VPNs for circumventing government controls, but politicians have expressed interest in cracking down on them in the past, including the arrest of four individuals for selling VPN services in 2013.[26] If the government makes VPN usage illegal and ISPs can track user connections to VPN providers, continued usage of this circumvention method may become more dangerous for protestors.

Future Circumvention of Iranian Government Censorship

Activists in Iran will have to consider two different environments when attempting to circumvent government censorship and control: standard connectivity via the NIN and isolation of the NIN from the rest of the world. The population typically experiences the first situation in non-tumultuous times. The current methods of government circumvention such as VPNs and anonymization networks should continue to facilitate activist communication, but the standing posture of the NIN may become more restrictive over time as it adds more capability, and the government creates additional legal restrictions. Since the NIN has demonstrated the capability to disconnect from the Internet in times of turmoil, dissidents will have to utilize different options for coordinating and using digital communications. If the standard posture of the NIN becomes sufficiently restrictive, it will force Iranian protestors to use similar options, regardless of whether the NIN is isolated.

Iranians mostly use VPNs to circumvent censorship. Since VPN connections are encrypted and effectively give the user an international intermediary system to connect to the Internet, users can circumvent government controls. However, this requires that users trust the VPN provider, since the intermediary system can see their traffic. Additionally, reliable and trustworthy commercial VPN providers require fees.

The viability of VPNs as a solution will probably become more complex, but should remain effective as long as the NIN remains connected to the Internet. The use of VPNs does not appear to be illegal at this time, but the selling or promotion of VPN services is considered criminal activity.[27] On the technical side, restricting VPNs can be difficult. The Ahmadinejad administration failed in its efforts to implement tighter controls on VPNs.[28] Attempts at stopping VPN connections by blocking their associated standard ports has limited effectiveness. Many commercial providers offer VPN connections tunneled through other protocols or ports so that these connections blend in with normal traffic. Authorities may also attempt to stop VPN connectivity by blocking known domain names or IP addresses associated with commercial providers. Activists can often circumvent these blocks by utilizing lower profile providers, providers that frequently roll their associated IP addresses, or by creating a custom VPN using cloud provider services like Amazon Web Services or Microsoft Azure.[29]

In addition to VPNs, dissidents have used the Tor anonymization network, as seen in the 2018 protests. Tor can circumvent government controls by utilizing international intermediaries similar to VPN services, but the intermediaries are voluntary and not controlled by a central entity or commercial company. Normal Tor usage requires a user to connect to a public directory to obtain a list of nodes for the user to connect to a Tor relay. In the past, the Iranian government has blocked access to the directory to prevent Tor usage.[30] To bypass this shortcoming, Tor offers "bridges" that are excluded from the public directory to enable users to make the first connection into a chain of Tor relays.[31] The necessity to obtain and use bridges adds another obstacle for users and may inhibit dissidents from using Tor.

If the NIN is isolated from the Internet, dissidents will have increased trouble with accessing uncensored digital communication. The best alternative would be to find an alternative communications channel from the normal ISPs. The most accessible, but possibly dangerous alternative would be to utilize domestic services in surreptitious manners to organize and share information.

Satellite communications offer a potential solution for an alternative means of connecting to the Internet. During the recent isolation event, the US ambassador to Germany stated that the United States and the European Union could "turn the Internet on" for Iran. Outside entities, whether governments or private organizations, could potentially provide satellite communication terminals from commercial companies such as Iridium or INMARSAT to trusted individuals inside the country. These solutions are constrained by relatively low bandwidth that could be quickly overwhelmed by video or high-quality image transfers. Future technical solutions such as SpaceX's Starlink satellite might offer more technically viable high bandwidth solutions. An additional problem is that the satellite terminals would be restricted to a small number of users inside the country and not effective as a means of mass organization.[32] Furthermore, because only terrestrial ISPs can legally provide access to the NIN and the Internet; mere possession of satellite terminals could be dangerous for protestors.

Mesh or peer-to-peer applications may provide a means of allowing uncensored coordination across groups. In the recent Hong Kong protests, dissidents have used an application called Bridgefy that uses BlueTooth functionality commonly found in phones to form a decentralized, ad hoc system known as a mesh network. Users can send messages to recipients across the city using the application while avoiding use of government-approved applications and communications channels. On the downside, these mesh applications currently have vulnerabilities. For example, mesh networks may be susceptible to monitoring by authorities since anyone can join the mesh. Additionally, the underlying protocols, such as BlueTooth and Wifi, have known vulnerabilities.[33] So far, these types of applications are a nascent capability; continued development may increase security against government monitoring.

In extreme cases, protestors may be able to utilize steganographic techniques over monitored communications systems such as the aforementioned Iranian domestic services to spread information and organize.[34] Steganography is the art or practice of concealing a message, image, or file within another message, image, or file. More simply, steganography is the art of hiding a message in a seemingly benign medium. An example of its use occurred in German spy messaging during World War II. The spies would write a benign message where the real message was embedded in the second letter of every word.[35] In the case of Iranian dissidents, they could use methods similar to that of the World War II spies to pass messages hidden as benign messages over monitored domestic services such as the Soroush (their Telegram clone). Protestors would need to coordinate on the channel for communication and an algorithm for hiding their hidden message. This complexity and requirement for prior out-of-band coordination would impede communicating with more than a small number of trusted users.

Conclusion

Iranian authorities have demonstrated a strong determination to prevent mass protest communications, such as what occurred in the Green Movement of 2009. The development of the NIN has enabled the government to increase monitoring and blocking. It also allows for the complete isolation of their domestic network from the global Internet in the event of extreme situations. Activists may have to resort to more complex and less widespread communications to overcome these countermeasures, but they should be able to sustain communications. While the NIN will greatly impede protest communications, it will likely not be able to fully prevent organization and messaging over digital networks.

Endnotes

[1] Luce, "Green Movement 2009."
[2] Gambrell, "Protests in Iran Fanned by Exiled Journalist, Messaging App."
[3] Calabrese, "Iranian Movement 'White Wednesdays' Finds Solidarity with U.S. Women's March."
[4] Erdbrink, "Tired of Their Veils, Some Iranian Women Stage Rare Protests."
[5] Madory, "Historic Internet Blackout in Iran."
[6] "Iran ISPs Ranked by Quality."
[7] "Iran."
[8] Xynou and Filasto, "Iran Protests: OONI Data Confirms Censorship Events (Part 1)."
[9] Bjorksten, "How to Help #KeepItOn in Iran."
[10] "After the Green Movement: Internet Controls in Iran, 2009-2012.", 10-11
[11] "Internet in Chains: The Front Line of State Repression in Iran.", 30
[12] "After the Green Movement: Internet Controls in Iran, 2009-2012.", 4-7
[13] Xynou and Filasto, "Iran Protests: OONI Data Confirms Censorship Events (Part 1)."
[14] Evdokimov, "Iran Protests: DPI Blocking of Instagram (Part 2)."
[15] Xynou, "Internet Censorship in Iran: Network Measurement Findings from 2014-2017."
[16] Xynou and Filasto, "Iran Protests: OONI Data Confirms Censorship Events (Part 1)."
[17] Madory, "Historic Internet Blackout in Iran."
[18] Cuthbertson, "Iran Shuts Down Internet Amid Protests, Leaving Country 'Isolated from the World.'"
[19] "Iran."
[20] "Iran: Government Surveillance Capacity and Control, Including Media Censorship and Surveillance of Individual Internet Activity.", 6
[21] Kargar, "Iran's National Information Network: Faster Speeds, but at What Cost?"
[22] Kargar.
[23] "Iran."
[24] "Query Response on Iran: Capacity and Methods of Authorities to Monitor Online Activities and Religious Activities of Iranians Living Abroad [a-10098]."
[25] "Tightening the Net: Internet Security and Censorship in Iran Part 1: The National Internet Project.", 43
[26] "Revolution Decoded: Iran's Digital Media Landscape" (Small Media and Arab Media Report, n.d.), https://smallmedia.org.uk/revolutiondecoded/a/RevolutionDecoded.pdf, 32
[27] "Iran."
[28] "Tightening the Net Internet Controls during and after Iran's Protests.", 11
[29] Crawford, "How to Bypass VPN Blocks - A Guide."
[30] Xynou and Filasto, "Iran Protests: OONI Data Confirms Censorship Events (Part 1)."
[31] "What Is Tor?"
[32] Schmidt, "How the US and EU Could Facilitate a Free Internet for Iran."
[33] Wakefield, "Hong Kong Protesters Using Bluetooth Bridgefy App."
[34] "Steganography."
[35] Leung, "Intoduction to Steganography."

BIBLIOGRAPHY

"After the Green Movement: Internet Controls in Iran, 2009-2012." Opennet Initiative, February 2013. https://opennet.net/sites/opennet.net/files/iranreport.pdf.

Bjorksten, Gustaf. "How to Help #KeepItOn in Iran." Access Now, January 10, 2018. https://www.accessnow.org/help-keepiton-iran/.

Calabrese, Erin. "Iranian Movement 'White Wednesdays' Finds Solidarity with U.S. Women's March." *NBC News*, January 21, 2018, sec. US News. https://www.nbcnews.com/news/us-news/iranian-movement-white-wednesdays-finds-solidarity-u-s-women-s-n839506.

Crawford, Douglas. "How to Bypass VPN Blocks - A Guide." Wirral, United Kingdom: ProPrivacy, January 14, 2019. https://proprivacy.com/vpn/guides/how-to-bypass-vpn-blocks.

Cuthbertson, Anthony. "Iran Shuts Down Internet Amid Protests, Leaving Country 'Isolated from the World.'" *Independent*, November 19, 2019, sec. INDY/LIFE. https://www.independent.co.uk/life-style/gadgets-and-tech/news/iran-internet-shutdown-protests-us-sanctions-a9209416.html.

Erdbrink, Thomas. "Tired of Their Veils, Some Iranian Women Stage Rare Protests." *New York Times*, January 29, 2018, sec. Middle East. https://www.nytimes.com/2018/01/29/world/middleeast/head-scarf-protests-iran-women.html.

Evdokimov, Leonid. "Iran Protests: DPI Blocking of Instagram (Part 2)." Open Observatory of Network Interference, February 14, 2018. https://ooni.org/post/2018-iran-protests-pt2/.

Gambrell, Jon. "Protests in Iran Fanned by Exiled Journalist, Messaging App." *AP News*, December 31, 2017. https://apnews.com/78a46cea167e4f94ada0a690b7f2f3db/Protests-in-Iran-fanned-by-exiled-journalist,-messaging-app.

"Internet in Chains: The Front Line of State Repression in Iran." New York City, NY: International Campaign for Human Rights in Iran, November 2014. https://www.iranhumanrights.org/wp-content/uploads/Internet_report-En.pdf.

"Iran." Freedom on the Net 2018. Washington DC: Freedom House, 2018. https://freedomhouse.org/report/freedom-net/2018/iran.

"Iran: Government Surveillance Capacity and Control, Including Media Censorship and Surveillance of Individual Internet Activity." Immigration and Refugee Board of Canada, January 16, 2015. https://www.justice.gov/sites/default/files/pages/attachments/2015/12/07/irn104972.e.pdf .

"Iran ISPs Ranked by Quality." *Financial Tribune*. March 7, 2017. https://financialtribune.com/articles/economy-sci-tech/60971/iran-isps-ranked-by-quality.

Kargar, Simon. "Iran's National Information Network: Faster Speeds, but at What Cost?" Cambridge, MA: Internet Monitor, February 21, 2018. https://thenetmonitor.org/bulletins/irans-national-information-network-faster-speeds-but-at-what-cost.

Leung, K. Ming. "Intoduction to Steganography." Polytechnic University - Department of Computer and Information Science, November 11, 2004. http://cis.poly.edu/~mleung/CS4744/f04/misc/steganography.pdf.

Luce, Mark David. "Green Movement 2009." *In Conflict in the Modern Middle East: An Encyclopedia of Civil War, Revolutions, and Regime Change*, edited by Jonathan Zartman. Santa Barbara, CA: ABC CLIO, 2019.

Madory, Doug. "Historic Internet Blackout in Iran." *Cisco Internet Intelligence* (blog), November 18, 2019. https://blogs.oracle.com/internetintelligence/historic-internet-blackout-in-iran.

"Query Response on Iran: Capacity and Methods of Authorities to Monitor Online Activities and Religious Activities of Iranians Living Abroad [a-10098]." ACCORD – Austrian Centre for Country of Origin and Asylum Research and Documentation, June 12, 2017. https://www.ecoi.net/en/document/1402692.html.

Schmidt, Fabian. "How the US and EU Could Facilitate a Free Internet for Iran." *Deutsche Welle*, November 11, 2019, sec. Science. https://www.dw.com/en/how-the-us-and-eu-could-facilitate-a-free-internet-for-iran/a-51313314.

"Steganography." Merriam-Webster. Accessed November 30, 2019. https://www.merriam-webster.com/dictionary/steganography.

"Tightening the Net Internet Controls during and after Iran's Protests." London, UK: Article 19, March 2018. https://www.article19.org/wp-content/uploads/2018/03/Tightening-the-Net-Internet-controls-during-and-after-Iran%E2%80%99s-protests_TTN-March-2018.pdf.

"Tightening the Net: Internet Security and Censorship in Iran Part 1: The National Internet Project." London, UK: Article 19, 2016. https://www.article19.org/data/files/The_National_Internet_AR_KA_final.pdf.

Wakefield, Jane. "Hong Kong Protesters Using Bluetooth Bridgefy App." *BBC News*. September 3, 2019, sec. Technology. https://www.bbc.com/news/technology-49565587.

"What Is TOR?" Electronic Frontier Foundation (EFF). Accessed November 30, 2019. https://www.eff.org/torchallenge/what-is-tor.html.

Xynou, Maria et al. "Internet Censorship in Iran: Network Measurement Findings from 2014-2017." Open Observatory of Network Interference, September 28, 2017. https://ooni.torproject.org/post/iran-internet-censorship/#facebook-messenger-test.

Xynou, Maria, and Arturo Filasto. "Iran Protests: OONI Data Confirms Censorship Events (Part 1)." Open Observatory of Network Interference, January 5, 2018. https://ooni.torproject.org/post/2018-iran-protests/.