global POLICY

Cyber Surveillance and Digital Authoritarianism in Iran

Shahram Akbarzadeh, Amin Naeni, Ihsan Yilmaz and Galib Bashirov
Alfred Deakin Institute for Citizenship and Globalisation, Deakin University, Australia

Abstract

The authoritarian regime in Iran has invested heavily in digital surveillance to identify and silence voices of dissent. Key institutions have emerged to develop new legal precedence, new technologies and new mechanisms of detection to capture cyber activists. Iranian authorities have learned from other digital authoritarian regimes, such as China, and have improved related technologies to exercise control over the internet and attempt to build a firewall around internet users in Iran. While dissident voices continue to be heard, the ruling regime has intensified its campaign of control in cyberspace. The battle over Virtual Private Networks (VPNs) is the latest episode in this digital authoritarian drive for control. The ruling regime's policies on cyberspace demonstrates its significance in the eyes of the authorities for the longevity of authoritarianism.

Policy Recommendations

- Western powers, particularly the US and the EU, should foster a framework of international collaboration among democratic nations and human rights and cybersecurity organizations to raise awareness about the pervasive surveillance system in Iran. Collaborative efforts should span mutually orchestrated research initiatives, foster the seamless exchange of crucial information, and support the strategic deployment of advocacy campaigns.
- International human rights organizations should initiate a proactive advocacy campaign to secure the recognition and robust protection of digital human rights in influential international forums. Western powers should help by leading the efforts to formalize the acknowledgment of fundamental rights, including online privacy and freedom of expression, as fundamental pillars in the digital realm.
- Digital authoritarianism is a growing global concern that is aided and abetted by the proliferation of censorship and surveillance systems. The EU should address this challenge by strategically supporting and amplifying the efforts of established and secure VPNs. By expanding access to these reliable tools, a broader spectrum of individuals in Iran can benefit from enhanced online privacy and circumvent digital surveillance.
- The United States and Canada should implement targeted sanctions directed at individuals and entities actively involved in the creation and sale of VPNs that contravene established human rights principles. This endeavour can start with identifying private enterprises collaborating with the Iranian regime to facilitate the expansion of surveillance systems, including those related to VPNs.

Over the past 20 years, developments in digital technologies have allowed states to dramatically elevate the scope and depth of their domestic surveillance capacity. The latter has allowed the state to monitor internet communications, collect information on individuals, and watch people's movements in urban environments. Managed by an expansive bureaucratic structure, such technological tools and practices have led to the emergence of surveillance systems worldwide. The COVID-19 pandemic has accelerated the use of surveillance technology across the world, adding force to the critical assessment of technology as not being neutral. In the context of China, for example, Chin and Lin have argued that surveillance technology has been put to the service of authoritarian rule for intrusive monitoring and data collection (Chin and Lin 2022). Research on surveillance systems has also explored innovative aspects in major cases such as China's Golden Shield Project (Chandel et al. 2019) and the Great Firewall (Griffiths 2021), Russia's Runet (Ermoshina et al. 2022), and the United States' National Security Agency (Greenwald 2014), while overlooking developing countries that have also built their surveillance systems with unique characteristics.

Iran is a poignant case of an authoritarian regime that has been building an expansive surveillance apparatus with technological and bureaucratic investment. Since the 2000s, the internet's widespread use has allowed the Iranian public to bypass state censorship. The internet was feared by the leadership and seen as a threat to state control. The Iranian authorities have invested in various censorship methods to control the physical and digital realms (Kawerau et al., 2022). However, censorship systems have been unable to tame cyberspace. From the 2009 Green Movement to the 2022 'Woman, Life, Freedom' movement, Iranian users have used the internet and, in particular, social media to raise their voices against the ruling autocracy. The Iranian regime's efforts at exercising control have encountered significant resistance; Iranian users have increasingly sought to circumvent censorship. This has prompted the government to develop a sprawling surveillance system to address the shortcomings of censorship measures. What are the peculiar characteristics of the Iranian surveillance system? What can it tell us about emerging surveillance systems in developing countries of authoritarian character? What are the implications for global policymakers and civil society whose goal it is to enable Iranian citizens to freely access the worldwide web?

This study examines this Iranian surveillance system. It first showcases the institutional design where the Supreme Council of Cyberspace (SCC) sits at the top of the institutional hierarchy, designing laws and policies to monitor Iranian citizens' online behaviour and restrict their digital freedoms. We then explore the role of the Cyber police (FATA) in monitoring Iranians' online behaviour and identifying dissident individuals. In addition, the Islamic Revolutionary Guard Corps (IRGC) is involved in actively flooding digital environments to manipulate online discourses through their cyber battalions. We then move on to discuss an innovative strategy employed by the Iranian regime wherein they utilize counterfeit Virtual Private Networks (VPNs) under their control to monitor and track users' online activities, steal sensitive data, and establish their real identities. As many Iranians resorted to using VPNs to circumvent harsh restrictions on internet access, the Iranian government invested in creating fake VPNs to deny Iranians such opportunities and instead attempted to steal their information. We also discuss how certain government actors abused this situation for economic gain by investing in creating and distributing fake VPNs, thus capitalizing on a lucrative market. Finally, we discuss the implications of the

Iranian case for global processes of authoritarian diffusion and the role of digital technologies in it.

This paper draws on primary and secondary data. The primary data includes interviews, official reports, and policy documents from Iran on institutional reforms, policy proposals, and state-market relations. The research team carried out 10 in-depth interviews via Zoom with relevant participants, including tech experts, digital and human rights activists, researchers, and journalists. Separate questionnaires were designed for participants in different categories to solicit the most relevant data in those interactions. Interviews took place during October 2022 - March 2023 over Zoom. The secondary data is drawn from Western and Iranian media reports and existing literature.

Institutions of Authoritarian Surveillance

Authoritarian regimes strategically allocate resources to acquire sophisticated digital tools customized for monitoring and analysing online activities. This empowers them to efficiently mitigate potential threats before their proliferation, thus safeguarding against potential adverse repercussions (Qin et al. 2017). The extensive and discreet monitoring of internet activities provides rulers with insights into citizens' online behaviour (Robbins and Henschke 2017). The implementation of online surveillance serves to bolster autocracy by amplifying the state's capability to exert coercive power, exemplified by the precise tracking of individuals of interest and their behaviour in cyberspace (Peterson and Hoffman, 2022).

Over the past 20 years, developments in digital technologies have allowed states to elevate the scope and depth of their domestic surveillance dramatically. The latter has allowed the state to monitor internet communications, collect information on individuals, and watch people's movements in urban environments. Managed by an expansive bureaucratic structure, such technological tools and practices have led to the emergence of elaborate national surveillance systems around the world. These systems can be used for various purposes, including national security, law enforcement, and social control. Some common components of these systems are CCTV infrastructure, facial recognition technology, AI and data analytics, internet censorship, monitoring and control centers, and bureaucratic institutions. As shown in the case of China, such a surveillance system is an integral part of authoritarian governance, whereby it enables the state to exercise control, maintain social order, and suppress dissent (Lilkov 2020).

Underpinning China’s massive system of surveillance is the vast bureaucratic infrastructure that not only manages and maintains the surveillance systems but also includes law enforcement institutions that identify, track, and control individuals or groups that may hold opposing political views or advocate for human rights and democracy. Two of the central pillars of this surveillance system are the Great Firewall and the Golden Shield Project. The former refers to an extensive system of censorship and internet surveillance involving a combination of legislative actions and technologies to regulate and restrict the country's internet space. It aims to block access to certain foreign websites and content that the Chinese government considers politically sensitive or harmful to its interests (Griffiths 2021). The Golden Shield Project is a broader initiative encompassing internet censorship and surveillance and the monitoring of electronic communications using technologies such as deep packet inspection or keyword filtering (Chendel et al. 2019). The project is not limited to internet censorship; it also includes efforts

to enhance the overall security and control of information within the country.

In Iran, the authoritarian regime has been building an expansive surveillance system that attempts to fuse technological and bureaucratic infrastructures. The Islamic Republic's attempts to control cyberspace have made it a pioneer of digital authoritarianism. The concept of digital authoritarianism was defined by Polyakova and Meserole as 'the use of digital information technology by authoritarian regimes to monitor, suppress, and manipulate both domestic and foreign populations' (2019, 1). Iran has now become a model of digital authoritarianism, and utilises a combination of censorship, disinformation, and extensive surveillance in the cyberspace to complement conventional measures of control over society (Conduit 2023). Digital authoritarianism not only restricts the flow of information but also attempts to disconnect online activities from offline developments. The 2009 Green Movement proved to be a milestone in the nexus between the cyber and the physical threat to the regime. Iranian protesters harnessed the power of social media platforms, such as Facebook and Twitter, to organize street rallies against the alleged election fraud (Golkar 2011). Access to social media has offered new opportunities for voices of dissent to be amplified (Khiabany and Zayani 2019).

Meanwhile, the Iranian government has increasingly expanded its authoritarianism from the physical to the digital realm. Supreme Leader Ali Khamenei's foundation of the SCC in 2012 marked a significant milestone in the expansion of digital authoritarianism in Iran. This influential body comprises high-ranking government officials, such as the president, representatives from the IRGC, the judiciary, and the parliament. It also includes select ministers such as defense, intelligence, and information and communications technology. Khamenei has tasked the SCC with the responsibility of devising, advancing, and monitoring security, legal, judicial, and police systems to promote regime control in cyberspace (Etemad Online 2015). As such, the SCC is the top bureaucratic organ that manages the Iranian surveillance system.

The SCC's desired objective is to build the National Internet Network (NIN) and separate Iran from the global network. Modelled after China's Great Firewall and Russia's Runet, the NIN will allow Tehran to claim national sovereignty in cyberspace and thwart all circumvention tools, such as VPNs (Entekhab 2019). In 2023, Gen. Ali-Akbar Ahmadian, Secretary of Iran's Supreme National Security Council (SNSC), stated that the US influences the governance of other countries through the internet, adding that 'cyberspace must solely be under the sovereignty of states' (Asr-e Iran 2023).

The NIN as the culmination of Iranian digital authoritarianism has received significant investment, but it is not yet completed (Financial Tribune 2023). As the regime has not been able to fully control cyberspace with conventional censorship methods, it has had limited success in controlling the relationship between online and offline activities. This was highlighted in the 2022 nationwide protests in Iran, where the internet helped to significantly expand the uprising following the killing of Mahsa Amini under the arrest of the so-called morality police. Iranian officials pointed to cyberspace as the main driver of the protests (Khamanei.ir 2022) and described the 2022 protests as the most dangerous 'riots' against the Islamic Republic (Khabar Online 2023).

These developments suggest that restrictive measures have failed to disconnect Iranian citizens from the internet. The shortcomings of the censorship system serve as a reminder to authorities that sustaining digital authoritarianism requires more than just censorship. This idea has been reinforced due

to the increase in social resistance against internet censorship. Amid the 2022 protests, Abolhassan Firouzabadi, the then Secretary of the SCC, acknowledged that the Iranian government did not recognize the right to anonymity of internet users, dismissing it as 'meaningless' (Digiato 2022). The 2022 'Woman, Life, Freedom' movement in the streets and online activism have served as a reminder to the authorities that state mechanism of control required greater investment and update to quell cyber activism.

Enhanced Surveillance

Iran is emulating China in developing and enhancing online surveillance tools. According to a draft of Iran's seventh development program presented in 2023, the Islamic Republic aims to significantly expand the capacity of its surveillance system within the next five years. Article 75 of this bill specifically refers to 'establish[ing] a continuous monitoring system for the indicators of people's lifestyle' and obliging database owners 'to furnish data to this system through online channels' (Ensaf News 2023). In a way similar to China's social credit system, the new system will put the personal lives of Iranian users under meticulous examination, with data processors gaining insights into detailed information such as users' location history, purchase records, travel routes, internet search history, and downloaded content. It will also allow the government to rank and categorize citizens and discriminate against them when providing public services and awards (Khabar Online, 2023). Moreover, transcending the sphere of policymaking, the Iranian regime has undertaken active efforts to elevate its surveillance capabilities by establishing relevant organizations and undertaking diverse projects.

An important component of the Iranian surveillance system is the Cyber Police, called FATA based on its Persian name. Established in early 2011, FATA is a specialized branch of the Iranian Police that is dedicated to addressing 'cyber-crimes' and has a significant role in surveillance (Mashregh News 2019). FATA is responsible for monitoring the cyber domain to identify dissident voices and arrest or silence them through harassment. Since its inception, FATA has played a significant role in identifying anti-regime activists online. In the words of Iran's police chief, Gen. Ahmad-Reza Radan, FATA's primary objective is to 'proactively identify and neutralize both current and future threats, ensuring a robust security posture' while using 'cutting-edge technology' (Fars News 2023).

One such cutting-edge technology is Deep Packet Inspection (DPI), which is a tool that inspects the data being sent over a network and may take various forms of actions, such as logging the content and alerting, as well as blocking or re-rerouting the traffic (Bendrath and Mueller 2011). Iran used its ties to China to acquire DPI technology. A Reuters report in 2012 revealed that China's ZTE Corp. sold DPI technology to the Iranian government at the estimated cost of $120 million. An Iranian insider claimed that the system could 'locate users, intercept their voice, text messaging ... emails, chat conversations or web access' (Stecklow 2012).

FATA assumes a pivotal role in monitoring online activities, discerning the identities of targeted individuals, especially dissidents amid protests, and subsequently apprehending them (Tasnim News 2019). There is no confirmed report on the number of forces in this police unit or their budget. However, in March 2022, the Iranian parliament enacted a decree imposing an obligation on Iranian banks and financial institutions to allocate two percent of their electronic transaction revenues to the national treasury. The designated funds are intended

to be utilized to reinforce FATA capabilities and improve its infrastructure (Digiato 2022).

Also, the IRGC has expanded its involvement in monitoring and controlling the internet, using the capacity of Basij forces – a paramilitary volunteer wing of the IRGC. In January 2017, Abdolsamad Khoramabadi, deputy to Iran's attorney-general at the time and a current member of the Supreme Court, reported that 18,000 volunteers had been recruited to survey 'counter-revolutionary' content in cyberspace. In November 2020, Mohammad Reza Yazdi, commander of Tehran's Mohammad Rasoulollah Corps, the biggest military unit in Iran responsible for crushing protests, reported the formation of 144 cyber battalions to counter the 'enemies' distortions' (Mehr News 2021). They appear to be part of the Cyber Army that is identified as an 'underground network of pro-regime cyber activists, hackers and bloggers [that] monitors the internet and launches cyber-attacks on opposition and anti-Islamic websites' (Robertson and Marchant 2018).

The IRGC mainly operates secretly in the cyber sphere, monitoring online interactions to suppress threats to the regime's authority and ideology. Its activities have been aided by a growing infrastructure of CCTV infrastructure in major Iranian cities by technology acquired from China's Dahua, Tiandy, and CETC (China Electronics Technology Group Corporation) (Stecklow and Rochabrun 2020). In 2018, Tehran Municipality signed an agreement with the latter to transform Tehran into a smart city. Other smart city projects are planned for Bushehr, Isfahan, Shiraz, and Mashhad (Nazari et al. 2021).

In addition, the Iranian government engages in undisclosed surveillance projects for which the responsible agencies remain unidentified. One such initiative has been the fabrication of counterfeit VPNs, which is unique to Iran. This endeavor facilitates the surveillance of internet traffic among unsuspecting Iranian users.

Fake VPNs in Iranian surveillance

VPNs were originally designed to safeguard users' online privacy by encrypting their internet traffic and circumventing internet censorship. Over the years, the strict censorship regime has made it necessary for Iranian internet users to use VPN services if they want to access the internet. Today, almost 80 percent of Iranian internet users utilize VPNs, according to an Iranian MP citing government reports (RFE/RL 2022). Among the top 50 applications Iranians use on Google Play, 40 are VPNs (Didban Iran 2022). During the 2022 'Woman, Freedom, Life' protests, daily demand for VPNs increased by 3000 percent (Gold et al. 2022). As the number of VPN users increased, the Iranian regime started to restrict its use. In June 2012, FATA launched a crackdown by banning 'illegal' VPNs and harassing users. Following China and Russia's lead, the Iranian regime made the VPN ban official in 2022 by barring the use of unauthorized VPNs in the Internet Protection Bill (RFE/RL 2022).

Restricting VPN use is a part of the Iranian regime's strategy of denying Iranian users access to international webpages. In an interview, a cybersecurity expert and human rights activist who was once detained in Iran told the authors that:

'The Islamic Republic has two interconnected policies regarding VPNs. On the one hand, they try to severely disrupt safe and well-known VPNs, making them useless for Iranian users due to slow connection speeds and frequent disconnections. On the other hand, only authorized VPNs have the capability to access international internet gateways, rendering other VPNs ineffective.'

Nonetheless, in recent years, a more interesting development has taken place that demonstrated the extent of authoritarian reach in the Iranian cyber space when it was revealed that the Iranian regime has

orchestrated ‘fake’ VPNs to trick users and collect their information. VPNs can inadvertently become tools for governments seeking to monitor and control digital communications. Consequently, individuals using VPNs to access restricted content or communicate without fear of surveillance can find their activities closely monitored. Iran serves as a compelling example of how the proliferation of controlled and counterfeit VPNs is employed to bolster the surveillance apparatus.

In January 2023, a report surfaced about a monitoring application, EyeSpy, that was developed within Iran. Bitdefender, a Romanian cybersecurity company, revealed that EyeSpy-infused malware spies on the users of 20Speed VPN ‘via trojanized installers,’ jeopardizing online privacy by keylogging and stealing sensitive data such as documents, images, crypto-wallets, and passwords. Bitdefender offered a few ways to identify fake VPNs while emphasizing that ‘there’s no bulletproof way’ to do so. In this vein, they pointed out three key indicators: the provider’s reputation, ambiguous privacy policy, and lack of contact details in VPN applications (Constantinescu 2022).

While most fake VPNs have remained undetected, cybersecurity companies have increasingly attempted to highlight the threats from counterfeit VPNs. In November 2022, Kaspersky – a global cybersecurity and digital privacy company – uncovered SandStrike as a previously unknown Android espionage campaign. The company reported that a Persian-speaking religious minority, Bahá’í, was targeted via the distribution of a VPN app that contained highly sophisticated spyware that allowed ‘threat actors to collect and steal sensitive data, including call logs, contact lists, and also track any further activities of persecuted individuals’ (Kaspersky 2022).

Moreover, Google's Threat Analysis Group has warned that state-sponsored hackers have attempted to camouflage their malicious software as VPN applications and uploaded them to the Google Play store. One of the significant campaigns that the Threat Analysis Group closely monitored was orchestrated by state-sponsored hackers affiliated with Iran, known as APT35. In May 2020, it discovered APT35's endeavour to introduce spyware into the Google Play Store by disguising its malicious payload as a VPN app, mimicking the appearance of ExpressVPN. Once installed on a user’s device, this fraudulent app could illicitly acquire sensitive data, such as call logs, text messages, contacts, and location information (Spadafora 2021). In this vein, an activist who works with a well-known Iranian human rights organization emphasized that:

‘Tracking online data of Iranian users has afforded the Islamic Republic access to data that can potentially result in not only apprehending the intended targets but also enabling security forces to identify connections between the victims and other dissidents. Under such conditions, counterfeit VPNs have been a strategy for the Iranian government to steal users’ information.’

The task of determining the authenticity of VPNs and tracing their origins is a technical pursuit primarily undertaken by cybersecurity firms. Nevertheless, even for these companies, the process is challenging, exacerbated by the ongoing and continuous development of new VPNs. The Iranian government has not accepted responsibility for controlling and spreading fake VPNs. But it is widely understood that the authorities are complicit in the sale of counterfeit VPNs and harvesting data Mehrdad Veys-Karami, an Iranian MP, has acknowledged that ‘Contrary to common perception, employing a VPN does not equate to escaping control; rather, it involves entering the sphere of control wielded by security forces (Etemad 2021a).’ In September 2022, after admitting to using a

VPN himself, former president Mahmoud Ahmadinejad said that ‘those engaged in content censorship are often the very same people that market and provide VPN services’ (Etemad Online 2021b).

Broader Implications

The development and proliferation of surveillance systems, as seen in the case of Iran, indicate a diffusion of authoritarian practices globally. States, especially those with authoritarian regimes, may adopt similar surveillance strategies to maintain control over their populations. Moreover, the advancement in digital technologies has significantly expanded the scope and depth of surveillance capacities, enabling states to monitor internet communications, collect individual information, and track movements in urban environments.

The Iranian case also illustrates the development of an expansive surveillance apparatus in response to challenges posed by the internet and resistance to censorship. Fake and controlled VPNs have been developed by what some Iranian officials have termed the 'Mafia of VPNs within the government’ (Didban Iran, 2021). In fact, the Iranian government's use of fake VPNs for monitoring and data theft, has opened the door to corrupt practices. Some MPs have criticized the government's involvement in the VPN market and called for transparency (Fararu, 2024). It appears that individuals close to the ruling regime have taken advantage of the gap between public demand for internet access and official restrictions to develop their own VPNs for economic and security gains. These are not secure and there are open to information sharing with authorities. This has led to the intersection of surveillance with economic interests. This practice also raises concerns about corruption and misuse of digital technologies for profiteering by individuals close to the ruling regime. The use of counterfeit VPNs could represent an innovative strategy to monitor and prosecute cyber activism.

Policymakers and civil society need to be aware of the evolving landscape of surveillance technologies, especially in developing countries with authoritarian tendencies. Understanding the peculiar characteristics of surveillance systems can inform global strategies to address challenges related to digital freedoms and privacy.

Prof Shahram Akbarzadeh (PhD) is Deputy Director (International) at Alfred Deakin Institute for Citizenship and Globalisation, Deakin University, Australia, and Non-resident Senior Fellow at Middle East Council on Global Affairs (Doha). His book on the Middle East Politics and International Relations: Crisis Zone was listed in top 20 books to read in international relations.

Amin Naeni is a PhD researcher and Research Assistant at t at Alfred Deakin Institute for Citizenship and Globalisation, Deakin University, Australia, and a Fellow at the Center for Middle East and Global Order (CMEG). His work focuses on Iran including socio-political impact of digital technologies within the country.

Prof Ihsan Yilmaz is a Research Professor at Alfred Deakin Institute for Citizenship and Globalisation, Deakin University, Australia. He has led multinational grant projects on populism, religion and international relations, digital technologies and transnational repression.

Dr Galib Bashirov is an Associate Research Fellow at Alfred Deakin Institute for Citizenship

and Globalisation, Deakin University, Australia. His research examines state-society relations in the Muslim world and US foreign policy in the Middle East and Central Asia.

Funding: This research was funded by Gerda Henkel Foundation, AZ 01/TG/21, Emerging Digital Technologies and the Future of Democracy in the Muslim World.

Bibliography

Chandel, S., Jingji, Z., Yunnan, Y., Jingyao, S., & Zhipeng, Z. (2019, October). The golden shield project of china: A decade later—an in-depth study of the great firewall. In *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)* (pp. 111-119). IEEE.

Griffiths, J. (2021). *The great firewall of China: How to build and control an alternative version of the internet*. Bloomsbury Publishing.

Asr-e Iran. (2023). 'Secretary of Iran's Supreme National Security Council: the US influences governance of other countries by the internet and social media platforms,' July 24, https://www.asriran.com/fa/news/899714

Bendrath, Ralf, and Milton Mueller. 2011. 'The End of the Net as We Know It? Deep Packet Inspection and Internet Governance.' *New Media & Society* 13(7): 1142-1160.

Chin, J., & Lin, L. (2022). *Surveillance State: Inside China's Quest to Launch a New Era of Social Control*. St. Martin's Press.

Conduit, D. (2023). Digital authoritarianism and the devolution of authoritarian rule: examining Syria's patriotic hackers. *Democratization*, 1-19.

Constantinescu, V. (2022). 'How to Identify a Fake VPN,' *Bitdefender*, October 13, https://www.bitdefender.com/blog/hotforsecurity/how-to-identify-a-fake-vpn.

Didban Iran. (2021). 'Zarghami: Mafia of VPNs is working inside the government.' April 25, https://www.didbaniran.ir/fa/tiny/news-106322.

Didban Iran. (2022). '40 of the 50 Popular Iranian Apps on Google Play Are VPNs.' December 31, https://www.didbaniran.ir/fa/tiny/news-146703.

Digiato. (2022). 'Head of the National Centre for cyberspace: Meta's lack of response to Iran's letter foreshadows the implementation of legal filters on Instagram,' December 17, https://digiato.com/article/2022/12/17/providing-new-opportunity-meta-interact-islamic-republic

Digiato. (2022). 'The parliament allocated 2 percent of the bank's electronic transaction income to strengthen the FATA police,' February 28, https://digiato.com/article/2022/02/28/cyber-police-share-banking-transactions.

Digiato. (2023). 'Member of Parliament: The annual turnover of filtering traders is more than 50 thousand billion tomans,' May 10, https://digiato.com/article/2023/05/10/annual-turnover-vpn-50-thousand-billion-tomans.

Ensaf News. (2023). 'A new protection bill in the seventh development?,' July 2, http://www.ensafnews.com/419088.

Entekhab. (2019). 'The implementation of the National Internet Plan Is Included in the 25-year Cooperation Document with China.' https://www.entekhab.ir/fa/news/572139/اجرای-طرح-اینترنت-ملی-در-سند-همکاری-۲۵-ساله-با-چین-آمده--است

Ermoshina, K., Loveluck, B., & Musiani, F. (2022). A market of black boxes: The political economy of Internet surveillance and

censorship in Russia. *Journal of Information Technology & Politics*, *19*(1), 18-33.

Esfandiari, G., & Zarghami, M. (2022). 'Iranian Vice President Under Scrutiny After Son Emigrates To Canada, Sells VPNs,' *Radio Free Europe/Radio Liberty*, September 13, https://www.rferl.org/a/iran-vice-president-son-vpns/32032030.html

Etemad Online. (2015). '10 duties and missions of the Supreme Council of Cyberspace in the new period', September 6, https://www.etemadnewspaper.ir/fa/Main/Detail/24618

Etemad Online. (2021a). 'Using VPNs means entering the sphere of control wielded by security forces,' December 28, https://www.etemadonline.com/tiny/news-529063

Etemad Online. (2021b). 'Ahmadinejad: I use VPN,' Etemad Online, March 25, 2021, https://www.etemadonline.com/tiny/news-473415

Fararu. (2024). 'Does the VPN mafia have influence in the government?' January 20, https://fararu.com/fa/news/701605.

Fars News. (2023). 'Neutralizing Threats: Future Architecture of FATA Police,' March 12, http://fna.ir/1ut293

Financial Tribune. (2023). 'Iran's National Information Network', July 22, https://financialtribune.com/tags/irans-national-information-network

Gold, A., McGill, M. H., & Rosenberg, S. (2022). 'Iran protests spark wider adoption of anti-censorship tools,' *Axios*, September 30, https://www.axios.com/2022/09/30/iran-protests-vpn-google-jigsaw-outline

Golkar, S. (2011). Liberation or Suppression Technologies? The Internet, the Green Movement and the Regime in Iran. *International Journal of Emerging Technologies & Society*, *9*(1).

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the US surveillance state*. Macmillan.

RFE/RL. (2022). 'About 80 Percent Of Iranians Use Tools To Circumvent Restrictions On Internet, MP Says'. https://www.rferl.org/a/iranians-circumvent-internet-restrictions/31933593.html

Kaspersky. (2022). 'New SandStrike spyware targets Android users with booby-trapped VPN application'. https://www.kaspersky.com/about/press-releases/2022_new-sandstrike-spyware-targets-android-users-with-booby-trapped-vpn-application

Kawerau, L., Weidmann, N. B., & Dainotti, A. (2023). Attack or block? Repertoires of digital censorship in autocracies. *Journal of Information Technology & Politics*, *20*(1), 60-73.

Khabar Online. (2023). 'Major General Salami: Last year's riots were the strongest and most dangerous global fight against the Islamic system of Iran', August 1, http://www.khabaronline.ir/xkhh5

Khabar Online. (2023). 'Monitoring all the data of Iranian users is on the agenda!,' July 1, https://www.khabaronline.ir/news/1784166

Khamanei.ir. (2022). 'Communication Platforms Have Now Become a Part of the War Strategy.' Personal website of Khamenei, November 9, https://farsi.khamenei.ir/others-dialog?id=51290 .

Khiabany, G., & Zayani, M. (2018). Citizenship and Cyber Politics in Iran. *Digital Middle East*, 217-238.

Lilkov, D. (2020). Made in China: Tackling digital authoritarianism. *European View*, *19*(1), 110-110.

Mashregh News. (2019). ‘What cases are investigated by the FATA police?,’ September 15, http://www.mshrgh.ir/992588

Mehr News. (2019). ‘Azeri-Jahormi's critique of the multi-billion-dollar trade network surrounding VPNs,’ September 2, http://www.mehrnews.com/xQ3r5

Mehr News. (2021). ‘3,500 cyber battalions are active within Basij,’ November 14, http://www.mehrnews.com/xWvMp

Nazari, V., Gholami, M., Fooladi, M. M., Majorzadehzahiri, A., & Alashkar, E. M. (2021). Smart city trend in Tehran. In *E3S Web of Conferences* (Vol. 263, p. 05052). EDP Sciences.

Peterson, D., & Hoffman, S. (2022). Geopolitical implications of AI and digital surveillance adoption. *Brookings Institution*.

Polyakova, A., & Meserole, C. (2019). Exporting digital authoritarianism: The Russian and Chinese models. *Policy Brief, Democracy and Disorder Series*, 1-22.

Qin, B., Strömberg, D., & Wu, Y. (2017). Why does China allow freer social media? Protests versus surveillance and propaganda. *Journal of Economic Perspectives*, *31*(1), 117-140.

Robbins, S., & Henschke, A. (2017). The value of transparency: bulk data and authoritarianism. *Surveillance & Society*, *15*(3/4), 582-589.

Robertson, B., & Marchant, J. (2014). Revolution Decoded: Iran’s digital landscape. *Small Media and Arab Media Report* *https://smallmedia.org.uk/revolutiondecoded/*

Shargh Daily. (2023). ‘The advice of the Minister of Communications: Do not use foreign free VPNs,’ July 10, https://www.sharghdaily.com/fa/tiny/news-887598

Spadafora, A. (2021). ‘State-sponsored attackers infiltrate Play Store with fake VPN app,’ *Techradar*, October 16, https://www.techradar.com/news/state-sponsored-attackers-infiltrate-play-store-with-fake-vpn-app

Stecklow, S. (2012). ‘Special Report: Chinese Firm Helps Iran Spy on Citizens’. *Reuters*. https://www.reuters.com/article/us-iran-telecoms-idUSBRE82L0B820120322

Szeles, J. B., & Botezatu, B. (2023). ‘EyeSpy - Iranian Spyware Delivered in VPN Installers,’ *Bitdefender*, January 11, https://www.bitdefender.com/blog/labs/eyespy-iranian-spyware-delivered-in-vpn-installers

Tasnim News. (2019). ‘31 leaders of recent riots in cyberspace were arrested in Hormozgan,’ November 30, https://tn.ai/2149892