Iran's Digital Authoritarianism as the Blueprint for National Sovereignty

Eleni Kapsokoli
University of Piraeus, School of Economics, Business, and International Studies,
Department of International and European Studies, Piraeus, Greece
Laboratory of Intelligence and Cyber-Security, Department of International and European Studies of the University of Piraeus, Greece

ekapsokoli@unipi.gr
ekapsokoli89@gmail.com

Abstract: As the technological landscape undergoes continuous transformation, nations are seizing the combination of technology, governance, and sovereignty in their strategies. Following the Arab Spring, a movement primarily focused on overthrowing oppressive regimes in the Middle East, Iran took a distinctive turn by establishing a digital authoritarian model. Fueled by concerns stemming from democratic reforms worldwide - especially those facilitated by the Internet and social media, which have played a pivotal role in the collection and dissemination of information - the Iranian government perceived a potential threat to its national security and sovereignty as well as its political survival. In response to the above, Tehran implemented a range of strategies and measures in Internet governance, which represent a form of oppressive control. To regulate the Internet and control the flow of data, Iran established the National Information Network, known as the 'Halal Internet'. This effort aims to safeguard national sovereignty through persistent control, shield political ideology, and promote a particular religious behavior within cyberspace. These developments have a noteworthy impact on individual rights, liberties, and privacy. This paper aims to explore the methods through which Iran exercises digital authoritarianism.

Keywords: Iran, Digital Authoritarianism, Sovereignty, Internet Fragmentation, Censorship, Surveillance.

1. Introduction

In an era marked by technological advancements, the intersection between governance, authority, and cyberspace has become increasingly pivotal. In recent years, there has been a growing trend among nations, seeking to enhance their national security and sovereignty, through the deployment of technology. Issues such as digital surveillance, information control, online censorship, law enforcement measures, the use of artificial intelligence and manipulation of big data can pose threats to human rights. This trend is facilitated by the swift digitalization of modern societies and is primarily orchestrated by state actors.

Many nations have (mis)used digital technology in the name of national security, leading to violations of (digital) rights and freedoms. The adoption of emergency security measures not only weakens democratic processes and regulatory structures but also leads to legitimizing authoritarian practices. Belarus, China, Iran, Russia, North Korea, and Saudi Arabia are notable examples of extensive censorship which significantly limits online access, thus violating people's right to information and communication. Other states such as the USA, France and the UK have used cyberspace to monitor their citizens, either for reasons of national security (terrorism, homeland security, pandemics, etc.) or to preserve and promote democracy. This trend has triggered numerous debates regarding the efficacy of using technology to galvanize national security and sovereignty. The emergence of authoritarian strategies by states in cyberspace imposes numerous constraints on fundamental rights such as privacy, freedom of speech, and political participation.

Among the states that (mis)use technology to hold power, Iran stands out as a distinctive one. Its path towards digital authoritarianism has unfolded due to geopolitical tensions, economic challenges, socio-political reforms, and a deeply rooted historical and religious content. Iran is a unified Islamic republic with a Shiite Islamic political doctrine based on the Guardianship of the Islamic Jurist (Velayat-e Faghih). This doctrine centralizes all political and religious power to the Supreme Leader of the country, who is considered a Guardian Jurist (Kasra, 2019). After the Iranian Revolution in 1979, Iran established a theocratic regime, combining propaganda and censorship, to exercise political control.

Over the past decades, Iran has witnessed periods of political and social conflict and protests, such as the Green Movement (2009) and the Arab Spring (2011) (Syed, 2022). The rule by Iranian radical clerics has resulted in restrictions on citizen's freedoms and rights and discrimination against minorities. Breaches of government policies lead to severe punishments, including prosecutions, imprisonments, and executions of dissenters, who violate international human rights standards (Human Rights Watch, 2023). The Iranian government responded to these protests by using the Internet for surveillance and repression purposes. A notable recent incident

illustrating this authoritarianism occurred in the autumn of 2022 during the intense protests over the tragic demise of Mahsa Jina Amini by the "Morality Police", for not adhering to hijab regulations (Rahimpour, 2022). This protest stands as the latest in a long struggle for civil rights and social justice (Bayat, 2022). These violations extend to the digital sphere, with the imposition of oppressive measures, such as surveillance, censorship, and hacking.

This paper aims to examine Iran's shift towards a digital authoritarian model to safeguard its national sovereignty and ensure its religious and political survival. The analysis begins with unveiling the layers of Iran's digital governance model, shedding light on the measures through which the regime utilizes technology to govern society. From surveillance technologies to control of information and cyber strategies, this paper aims to deepen our understanding of how the Iranian government shapes its political landscape using a digital toolbox to ensure national authority. Additionally, it examines the implications of these practices on the Iranian population and considers their broader impact on the international community. The paper concludes by highlighting the exchange of best practices and means between Iran and other digital authoritarian regimes.

2. Iranian Digital Authoritarianism

Iran has experienced a significant rise in digitalization in recent years, especially in terms of Internet usage and social media adoption. The statistics below highlight the growing influence of information communication technologies (ICTs) and cyberspace in Iranian society. From a total of 88.84 million, there are 69.83 million Internet users, which is essential for understanding the growth and engagement of its population with the Internet. Furthermore, the number of social media users reached 48 million in 2023, proving the existence of an active digital blogosphere (Kemp, 2023).

Despite undergoing a digital transformation, Iranians have experienced Tehran's effort to control cyberspace and social media, thus regulating the flow of information within society. It implemented restrictive measures to monitor and surveil information and activities. This country is one of the most active and formidable cyber actors in the Middle East region, with a growing and increasingly sophisticated set of capabilities. The analysis of the strategic use of ICTs for a range of objectives by Iran is depicted through the following figure with the title "Iran's Digital Authoritarian Model". This figure exemplifies the extensive and often malicious use of technology in the pursuit of national authority. It includes objectives such as censorship, surveillance, hacking, propaganda, filtering, and Internet fragmentation. This figure has a dual use. On the one hand, it aspires to monitor national security crises such as epidemics, acts of terrorism, military operations, and geopolitical challenges. On the other hand, it aims to restrict dissenters' voices because the Internet is the primary tool for promoting political views.

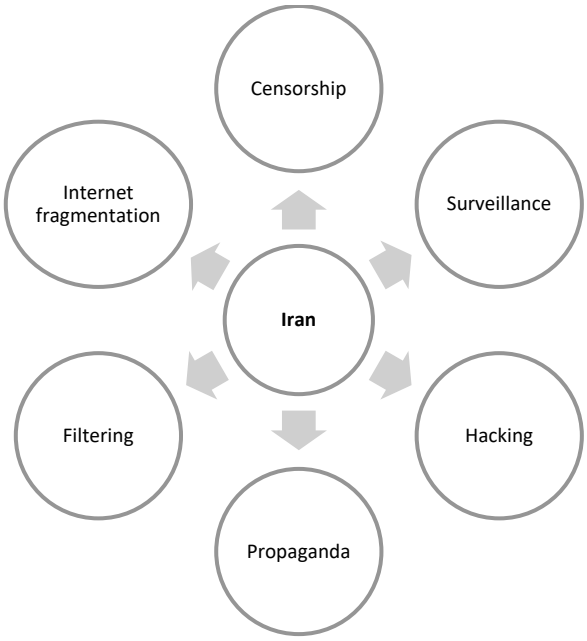

Figure 1: Iran's Digital Authoritarian Model

Specifically, the government exercises extensive and unrestrained censorship of users' online content, employing a sophisticated filtering system to block access to websites, news outlets, and social media platforms that criticize

the government. On June 27, 2023, Khamenei requested the judiciary to act in 'purging' dissenting voices from the Internet, for the protection of public rights, the preservation of societal psychological safety, and the suppression of violations and crimes (Article 19, 2023). According to Freedom House's annual report of Internet Freedom, covering the period from June 2022 to May 2023, Iran experienced a significant decline in its score, dropping 5 points. This decline resulted in the country securing the third lowest ranking, with an overall score of 11 out of 100 (Freedom House, 2024). This underscores that the very technology can contribute to societal development and can also be employed to undermine it.

In addition, the government conducts strict surveillance using advanced software and artificial intelligence tools (algorithms and biometric features) to monitor mobile telephony and online activity. Another method involves the dissemination of online propaganda with disinformation campaigns and the creation of fake news by Iranian state and non-state actors. They manipulate social media platforms by creating troll accounts to influence public opinion with pro-government narratives. Iranian authorities provide citizens with access to specific news sources that reproduce fake news to promote Tehran's narratives. Iranian users cannot find information on Internet search engines that is against the Iranian government. The Iranian Constitution refers to freedom of expression and press, but news agencies enjoy these freedoms as long as their content does not oppose the political principles of Iran. Thus, Iran is ranked 177/180 in the World Freedom of Reporters without Borders (2024). For example, information related to the protests, the arrests and killings of dissenters, and the financial corruption of state actors, are blocked. Furthermore, the Iranian authorities provide access to carefully constructed and filtered information, or they reply to criticism by using disinformation and fake news (Martin, 2018). One example is the dissemination of a video by the Tehran police to defend the official version of the cause of death of Mahsa Amini. This video claimed that Masha Amini had died of a heart attack and was not murdered by the Iranian morality police (NPR, 2023). Iran's digital toolbox is further complemented by the implementation of a sophisticated filtering system, which controls the flow of online information.

Since 2012, Tehran has been trying to establish its national Internet, referred to as the National Information Network [also known as SHOMA, or Internet-e Paak (Pure Internet), or Halal Internet (Permitted or Lawful Internet)]. The primary objectives of the Halal Internet include the improvement of speed connectivity, safeguarding information, hindering international surveillance, and developing cyber-defence capabilities against malicious cyber activities. The main idea is to create a 'clean' network that does not need censorship and protects citizens from moral hazards. It is envisioned as a locally controlled version of the Internet (Free Word Centre, 2016). The fragmentation and localization of the Internet offers Iran the means to control its digital frontiers, while at the same collecting citizens' metadata within local information infrastructures (Hendrix, 2022). In this National Information Network, all users are identifiable through a single and unique digital identifier, enabling the state to determine the content that users are allowed to access. The government is trying to de-westernize Iranian society, by prohibiting fashion, music, and pornography, thereby strengthening national sovereignty. Although the government promotes the adoption of the National Information Network, citizens remain skeptical. This skepticism stems from the recognition of its purpose, which is to impose stricter surveillance and censorship. In the pursuit of this agenda, the government is trying to develop and promote local communication platforms and strengthen the operation of this information infrastructure. Iranians face the following dilemma. Either sacrificing their privacy and anonymity, but gaining better connectivity, greater cybersecurity measures and low-cost services within the National Information Network or remaining digitally isolated. Many Iranians have found ways to bypass the restrictions of the National Information Network, with proxy servers (such as virtual private networks - VPNs) to hide their Internet Protocol (IP) addresses and geolocation while maintaining anonymity (OONI, 2022). This trend has resulted in a continual hide-and-seek game between the government and the citizens, with the former implementing ever-increasing censorship and surveillance techniques, and the latter trying to express their voice their dissent and resist these measures.

Iran's digital architecture consists of distinct entities with varying responsibilities and decision-making authority, engaging in both defensive and offensive cyber activities. To begin with, the Supreme Council of Cyberspace (SCC) was established in 2012 to employ decisions related to the governance of the Internet. Serving as an extension of SCC, the National Center of Cyberspace (NCC) focuses on information content and the development of security measures. The Iranian Cyber Police (Fata), established in 2011, has a responsibility to counter cybercrime and cyber threats that compromise national security. The Ministry of Information and Communications Technology has as a task the formulation and implementation of policies and measures concerning technology development and usage. The Ministry of Intelligence and Security (MOIS) is responsible for the flow of information, by collecting and processing intelligence derived from electronic communications. Operating within the Armed Forces, the Islamic Revolutionary Guards Corps (IRGC) oversees offensive cyber activities. A part of IRGC is the

Electronic Warfare and Cyber Defense Organization (IRGC EWCDO), which provides essential training to personnel to develop cyber-defence, surveillance, and censorship capabilities. The Basij Cyber Council (BCC) consists of volunteer hackers actively engaging in conducting malicious cyber activities. The defensive digital front includes the National Passive Defense Organization (NPDO) and Cyber Defense Command (CDC), which strengthen the state's cyber resilience. The Working Group to Determine Criminal Content (WGDCC) is responsible for detecting illegal content and informing the Center to Investigate Organized Crime (CIOC), which proceeds with the arrest of users who post content against the Iranian government. Moreover, the Communications Regulatory Authority (CRA) was established in 2003 and is responsible for regulating the telecommunications sector. Finally, the Iran Legal Intercept System (ILIS) constitutes a mechanism for surveillance and regulation of cyber activities. It gathers data about individual's mobile services which can modify or terminate their access (Center for Human Rights in Iran, 2015; Access Now, 2023). Within this System, there are some sub-entities, including the Control Illegal Devices (CID) System which issues warnings regarding the change of unauthorized SIM cards and the SHAHKAR System, which is designed for the collecting of audio data from mobile users and detecting cases of tampering (Miller et al, 2023).

Tehran has facilitated its ability to control the Internet and surveil the online behavior of Iranians by using espionage software like SIAM, SecondEye and EyeSpy (Alimardani, 2023, 9). SIAM can execute remote forty commands such as the ability to engage in online activity monitoring; to decrypt, collect, and process data; to do geo-location; to slow down Internet connectivity; to track the physical movements of individuals or large individuals; and to restrict access to dissenters. The 'Forge2GNumber' command, enables the degradation of network quality and speed connectivity from 4G and 3G to 2G (Zetter, 2020). Such a decline makes connections extremely vulnerable, making smartphones and high-tech applications useless, while compromising the personalization and privacy of data due to the absence of encryption. Therefore, Iranian authorities can easily collect, process, and store data, given the increased exposure of information at 2G speeds. SIAM's 'GetCDR' command facilitates the categorization of data, resulting in the creation of a personalized profile for each citizen. The data collected including information such as names, family details, passport information, IP addresses, phone-related data, etc. – contributes to a strategic advantage for the Iranian authorities during surveillance and censorship of cyberspace. The 'LocationCustomerList' command permitted the tracking and identification of mobile phone users based on their physical movements (Intercept, 2022). Telecommunications entities in Iran - including Ariantel, Telecommunication Company of Iran (TCI), Mobile Communications Iran, MTN Irancell, Rightel, and Shatel - install SIAM on citizens' mobile phones, thereby granting authorities full access to essential information (Bushwick & Bose, 2022). Bypassing the SIAM surveillance program cannot be achieved through simplistic solutions such as changing the SIM cards.

Tehran has manipulated hacking groups that are state-sponsored and engage in cyber espionage for various purposes, including gathering intelligence from foreign or domestic entities, monitoring geopolitical developments, and supporting national interests (e.g. gathering scientific knowledge). Examples of these groups are the APT33 (Elfin, Rocket Kitten, or Refined Kitten), APT34 (OilRig or Helix Kitten), APT35 (Charming Kitten, Newscaster, or NewsBeef), Tahr Andishan (The Thinkers) and APT39 (Chafer). For example, in retaliation for the Stuxnet computer virus on Iranian nuclear facilities, Iranian hacking groups conducted large-scale cyberattacks on the national critical infrastructure of foreign states, such as the Saudi Arabian Oil Company and the Shamoon virus (Gambrell, 2018B). Another significant cyberattack was against the Technical University of Denmark in March 2018. Hackers gained illegal access to several research projects to be used to enhance Iran's scientific knowledge across different fields. The US authorities reported in 2018, that nine Iranian hackers were accused of cybercrime by targeting 320 universities in 22 countries (Saikal & Vestenskov, 2020*,* 18–30). These actions highlight Iran's strategic use of cyber espionage to gather scientific knowledge.

3. Iran Suppresses Digital Rights

The Iranian government has witnessed a rise in public protests motivated by a spectrum of socio-political grievances. The Green Movement and Arab Spring highlighted the dynamic and direct impact of social media in shaping socio-political situations and narratives, thereby enhancing the online presence of Iranians. Activists organized the Green Movement by using platforms like Twitter and Telegram. During these protests, Iranian authorities prevented the 'Twitter revolution' by banning the app (Liaropoulos, 2013, 8). The oxymoron is that Ahmadinejad, the orchestrator of this ban, was a Twitter user. This app proved to be valuable for the dissemination of information, primarily orchestrated by foreign citizens and journalists in other foreign languages and not in local dialects, thus attracting the attention of a global audience (Keller, 2010).

In the aftermath of the Arab Spring, Iranian authorities adopted a dual approach to counter the scope of the demonstrations and control the narratives. The first approach is to monitor online activities and censor content as politically sensitive or unlike within its ideological and religious standpoint. In this context, Tehran employed methods such as the filtering and blocking of websites, messaging applications, and social media platforms, where individuals express dissenting socio-political perspectives and engage in online political activism (Gambrell, 2018A). Iran spent 36 million dollars in 2016 to develop 'smart filtering' technology that would allow authorities to selectively censor its citizens' Internet access (Cuthbertson, 2018). They also forbid two-step verification codes which are essential to using some online services or social media (RadioFreeEurope, 2022).

An important example is the prohibition of Telegram on December 31, 2017, following the decision of its CEO, Pavel Durov, to refuse to deplatform the peaceful protest channels. These channels provided the possibility of encrypted communication and coordination for the protests as well as the dissemination of audio-visual material that testified to the use of force by the Iranian authorities (BBC News, 2018). Durov criticized Tehran's decision and hashed measures, stating that Telegram is used by thousands of major opposition channels around the world and that freedom of speech is an undeniable human right. A few months later, Khamenei deactivated his personal Telegram account to protect national security.

Concurrently, Iranian authorities employ sophisticated tactics to manipulate social media narratives through disinformation campaigns and fake news to distort confusion and polarization and affect public opinion. Troll accounts are used to promote state-sponsored propaganda, suppress dissenting voices, and create a new online socio-political reality. By blocking the counter-narratives in cyberspace, the Iranian government seeks to shape both domestic and international perceptions of the inside policy. They also developed regional social networking and communication platforms, such as Soroush and Gap, resembling Instagram and Telegram, to replace them (McDermott, 2022). Iranian authorities have closely monitored these platforms to censor and control their users. However, these apps were not very successful, as users were aware of the potential risks that they posed to their privacy and security (Article 19, 2018).

Numerous women have opposed the restrictive legislative measures and obligatory hijab requirements, engaging in protests to voice their dissent. After these protests, in September 2022, the Headquarters for the Promotion of Virtue and the Prevention of Vice announced the adoption of artificial intelligence facial recognition technologies with biometric features for women who do not comply with regulations regarding the use of hijab (Shakibi, 2022). It is the first known case of a government using facial recognition to impose dress laws on women based on religious beliefs. Incidents have emerged wherein women are being notified via text messages or emails about violations, detected by traffic cameras, social media, and personal data from their phones. Between April till June 2023, more than one million warning messages through the Najer program were sent to women found without hijab in public spaces or on social media, or those displaying nudity or wearing thin or tight clothing (Amnesty International, 2024). Women, who are considered lawbreakers, face severe consequences, including the denial of access to financial institutions, public transportation, employment, health care and other basic government services. Furthermore, such violations may lead to prosecutions or morality training. The implementation of these measures has been exacerbated following the adoption of the Hijab and Chastity Bill in September 2023, which further intensifies penalties for women who either do not follow hijab requirements or promote relevant protests (Alimardani, 2023, 9).

The second approach includes constraints of Internet accessibility and shutdowns (Article 19, 2022). Iran has had a series of incidents with Internet shutdowns during periods of high unrest. By disrupting the Internet, the government aims to hinder communication among protesters and the organization of the protests and to control the dissemination of information. During these shutdowns, citizens are in a state of digital isolation, unable to communicate and to have access to news. Notably, during the November 2019 protests, the Internet remained offline for ten consecutive days. Iranian authorities effectively targeted protests by knowing their location and organizational information. In the protests of autumn 2022, they shut down the Internet for at least one week. During this period, there was a systemic violation of human rights and freedoms with arrests and executions, specifically, more than 14,000 civilians were arrested, and 300 civilians were executed (Amnesty International, 2023).

The general perception of the government regarding the usage of cyberspace by citizens is confirmed by Khamenei's statement that the Internet is being used by the enemy to target Islamic thought and the Islamic way of life. Based on the above perception, Tehran introduced in July 2021, the 'Regulatory System for Cyberspace Services Bill' (Tarhe Sianat), which enhances oppression in Iran. This Bill is a set of regulatory restrictions on rights and freedoms that aim to digitally isolate and fully control the flow of data and services (Article 19, 2021). It

criminalizes the use of VPNs and imposes strict regulations on social media and technology companies. These companies are required to align with government standards, including access and storage of metadata to local information systems (Motamedi, 2019). The Bill empowers the Committee Charged with Determining Offensive Content (CCDOC) to take drastic actions against companies that resist collaboration with authorities. This includes the possibility of complete prohibition of activity, bandwidth limitations or imposition of economic sanctions (McDermott, 2022). Till now, Iran's Supreme Cyberspace Council (SCC), which was established by Khamenei in 2012, has seemingly adopted partial draconian measures of the Bill. If it is fully adopted, it will violate several human rights, and surveillance and censorship will be unhindered and limitless.

The above measures not only restrict the fundamental right of freedom of expression but also interfere with the citizens' right to access information and the right to peaceful assembly. The government seeks to silence opposition and maintain control. The Iranians have shown their dissatisfaction by increasing political activism and externalizing information about governmental violence. Moreover, Iranians are becoming more adaptable by identifying and countering disinformation campaigns and fake news and developing a sense of media literacy. In addition, the protesters have found alternative solutions to respond to these violations by using VPNs and encrypted messaging apps. Despite these collective efforts, the struggle for human rights and political change remains an unequal and difficult battle. Tehran aims to dominate within its physical borders by building a 'digital wall'.

4. Iranian's digital alliances

The imposition of economic sanctions by the United States on Iran has been notable, leading to economic and societal challenges, and public discontent. This economic pressure contributed to social unrest and protests as a response to both economic conditions and dissatisfaction with the political regime. The Iranian government has taken measures to control and suppress protests. Regarding the government's actions in response to sanctions, Tehran seeks alternative solutions and alliances to mitigate the effects. Cooperation with like-minded countries can be one effective strategy. Additionally, investing in technological capabilities and forming alliances with technologically superior actors are potential responses to sanctions.

China became Iran's primary technological ally, providing substantial support with intelligence monitoring and control, geolocation, espionage, and censorship systems. Since 2012, ZTE Company has signed a technology agreement with Iran to provide mobile geolocation and data interception equipment and software. In 2022, the Chinese company Tiandy Technologies further enhanced Iran's surveillance capabilities, by supplying closed-circuit cameras (Iran International, 2022). A pivotal development in Sino-Iranian relations happened in March 2021, when they signed the 'Iran-China 25-Year Cooperation Plan'. This Plan is a roadmap for trade, economic cooperation, military engagements, technological exchanges, and transportation initiatives, with a key emphasis on the private sectors of both entities. Beijing committed to invest more than 400 billion dollars in a period of 25 years, in all the aforementioned sectors, but mainly in telecommunications and technological ones by installing 5G networks. The bilateral cooperation emphasizes various domains such as long-distance communication equipment, 5G programs, ICT equipment, cybersecurity, artificial intelligence and browsing software and technology, and the exchange of practices and information between higher education institutions and technology companies (Azarhoosh, 2020). In a statement, an Iranian official has announced that Iran will launch 4.000 sites to provide 5G Internet services till March 2025 (Islamic Republic News Agency, 2023). China is systematically trying to penetrate the Iranian sphere and play a decisive regional role in an area of the Middle East. This geopolitical shift is a source of heightened apprehension for the USA, given their bilateral escalating relations, fueled by concerns over China's actions and their potential effect on the regional balance of power.

Another state that actively supports Iran and applies relevant strict measures in its society is Russia. Moscow has been providing Tehran since 2022, with advanced surveillance technologies, as part of their military and cyber cooperation. In exchange for military support that Iran had offered for the Ukrainian battlefield – Russia has supplied Tehran with advanced eavesdropping and photography devices, lie detectors and software for hacking mobile and information systems (Iran Wire, 2023). PROTEI Ltd, a Russian technology company, has enabled Iranian authorities to monitor, decrypt, redirect, degrade or deny all mobile communications of Iranians, by using software for online censorship (Miller et al., 2023). This collaboration between Moscow and Tehran extends beyond surveillance and espionage programs and aims at enhancing their capabilities to conduct cyber warfare (Lieber et al., 2023).

5. Concluding Remarks

Iran has transformed into a sophisticated surveillance, censorship, and hacking state. Instead of aligning its strategies and laws with international standards on human rights, accountability and freedoms, Iran has adopted harsher measures against its society. The Iranian government does not necessarily want to prohibit the Internet and the use of social media and platforms; rather, it seeks to 'purify' these means from any element that infects Iranians' loyalty and civic duties. Iran now possesses a digital toolbox that is capable of silencing and controlling its citizens, but also maintaining security and sovereignty.

The National Information Network does not guarantee anonymity, privacy, or data protection. Instead, authorities can filter or censor online content for any citizen. The status of net neutrality is compromised by regulations and strategies, content diversity is greatly reduced, and individuals are impeded from freely disseminating information. In the event of future protests, the government could resort to shutting down the Internet and blocking mobile communication, preventing Iranians from exchanging, gathering, and accessing information, as well as publicizing violent state incidents. Even if Iran is diplomatically isolated from the West, it maintains crucial ties with powerful allies such as China and Russia. It is imperative for the international community, human rights mechanisms, governments, and the technology sector not to remain passive, but to actively address these practices. Iranians deserve unhindered access to cyberspace and their fundamental rights should be intact.

Acknowledgements

This work has been partly supported by the University of Piraeus Research Center.

References

Access Now (7 March 2023) *Iran: Human rights groups sound alarm against draconian Internet Bill*. Available at: [Online] Iran: Human rights groups sound alarm against draconian Internet Bill - Access Now

Alimardani, Mahsa. (2023). 'Aggressive New Digital Repression in Iran in the Era of the Woman, Life, Freedom Uprisings', in *"New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms"*, edited by Steven Feldstein Steven, Carnegie Endowment.

Amnesty International (26 July 2023) *Iran: International community must stand with women and girls suffering intensifying oppression*. Available at: [Online] https://www.amnesty.org/en/latest/news/2023/07/iran-international-community-must-stand-with-women-and-girls-suffering-intensifying-oppression/

Amnesty International. (Last access 9 April 2024) *A web of Impunity: The killings Iran's internet shutdown hid*. Available at: [Online] A web of impunity: The killings Iran's internet shutdown hid — Amnesty International

Article 19 (21 October 2018) *Iran: National messenger apps are the new hallmark of Internet nationalization*. Available at: [Online] https://www.article19.org/resources/iran-national-messenger-apps-are-the-new-hallmark-of-internet-nationalisation/

Article 19 (4 November 2021) *Tightening the net: Alarming moves to enforce the "User Protection Bill"*. Available at: [Online] Tightening the net: Alarming moves to enforce the "User Protection Bill"

Article 19 (17 November 2022) *Iran: New tactics for digital repression as protests continue*. Available at: [Online] https://www.article19.org/resources/iran-new-tactics-for-digital-repression-as-protests-continue/

Article 19 (6 July 2023) *Iran: Supreme Leader orders judiciary to further restrict online freedoms*. Available at: [Online] https://www.article19.org/resources/iran-supreme-leader-orders-judiciary-to-further-restrict-online-freedoms/

Azarhoosh, K. (2020) *The Iran-China Partnership: A Bad Deal for Citizens and Tech Companies*, Investigations. Available at: [Online] https://filter.watch/en/2020/11/13/the-iran-china-partnership-bad-news-for-tech-companies-a-disaster-for-citizens-rights/

Bayat, A. (26 October 2022) *A New Iran Has Been Born — A Global Iran,* New Lines Magazine. Available at: [Online] A New Iran Has Been Born — A Global Iran - New Lines Magazine

BBC News (3 January 2018) *Iran protests: Telegram under fire as Tehran clamps down*. Available at: [Online] https://www.bbc.com/news/world-middle-east-42558317

Bushwick, S. and Bose, T. (4 November 2022) *What You Need to Know about Iran's Surveillance Tech*, Scientific American. Available at: [Online] https://www.scientificamerican.com/podcast/episode/what-you-need-to-know-about-irans-surveillance-tech/

Center for Human Rights in Iran (2018) *Guards at the Gate the Expanding State Control over the Internet in Iran*. Available at: [Online] EN-Guards-at-the-gate-High-quality.pdf (iranhumanrights.org)

Cuthbertson, A. (5 January 2018) *Iran Internet Censorship Forces Protesters to Turn to Dark Web*, Newsweek. Available at: [Online] https://www.newsweek.com/iran-internet-censorship-sees-protesters-turn-dark-web-772182

Free Word Centre (2016) *Tightening the Net: Internet Security and Censorship in Iran. Part 1: The National Internet Project*. Available at: [Online] The_National_Internet_AR_KA_final.pdf (article19.org)

Freedom House (Last access 9 April 2024) *Freedom on the Net 2023- Iran*. Available at: [Online] https://freedomhouse.org/country/iran/freedom-net/2023

Gambrell, J. (29 January 2018A) *'Halal' internet means more control in Iran after the unrest*, Associated Press. Available at: [Online] https://apnews.com/article/c02a320725fc4afda305a0f3a660dbe6

Gambrell, J. (4 February 2018B) *In Iran, a 'halal' internet means more control after unrest*, Arab Weekly. Available at: [Online] https://thearabweekly.com/iran-halal-internet-means-more-control-after-unrest

Hendrix, J. (17 November 2022) *Internet Shutdowns and Censorship, in Iran and Beyond*, Tech Policy Press. Available at: [Online] Internet Shutdowns and Censorship, in Iran and Beyond | TechPolicy.Press

Human Rights Watch (2023) *World Report 2023: Iran*. Available at: [Online] World Report 2023: Iran | Human Rights Watch (hrw.org)

Iran International (16 December 2022) *US Sanctions Chinese Video Surveillance Firm Supplying Iran*. Available at: [Online] US Sanctions Chinese Video Surveillance Firm Supplying Iran | Iran International (iranintl.com)

Iran Wire (28 March 2023) *Russia Provides Iran with Digital Surveillance Capabilities.* Available at: [Online] Report: Russia Provides Iran with Digital Surveillance Capabilities (iranwire.com)

Islamic Republic News Agency. (31 October 2023) *4,000 sites to provide 5G internet in Iran by March 2025.* Available at: [Online] https://en.irna.ir/news/85276210/4-000-sites-to-provide-5G-internet-in-Iran-by-March-2025

Kasra, A. (20 March 2019) *What Is Velayat-e Faqih?*, Tony Blair Institute for Global Change. Available at: [Online] https://www.institute.global/insights/geopolitics-and-security/what-velayat-e-faqih

Keller, J. (18 June 2010) *Evaluating Iran's Twitter Revolution*, The Atlantic. Available at: [Online] Evaluating Iran's Twitter Revolution - The Atlantic

Kemp, S. (13 February 2023) *Digital 2023: Iran*, Datareportal. Available at: [Online] https://datareportal.com/reports/digital-2023-iran

Liaropoulos, Andrew. (2013) "The Challenges of Social Media Intelligence for the Intelligence Community", *Journal of Mediterranean and Balkan Intelligence*, Vol 1, No 1.

Lieber, D., Faucon, B. and Amon, M. (27 March 2023) *Russia Supplies Iran with Cyber Weapons as Military Cooperation Grows*, The Wall Street Journal. Available at: [Online] Russia Supplies Iran With Cyber Weapons as Military Cooperation Grows - WSJ

Martin, A.J. (12 January 2018) *Iranian regime's 'halal' internet stifling protest*, News Sky. Available at: [Online] https://news.sky.com/story/iranian-regimes-halal-internet-stifling-protest-11202100

McDermott, G. (10 November 2022) *Iran's digital authoritarianism is being tested by the country's youth*, Prachatai English. Available at: [Online] https://prachataienglish.com/node/10087

Miller, G., Al-Jizawi, N., Ermoshina, K., Michaelsen, M., Panday, Z., Plumptre, G., Senft, A. and Deibert, R. (16 January 2023) *You Move, They Follow. Uncovering Iran's Mobile Legal Intercept System*, The Citizen Lab. Available at: [Online] You Move, They Follow: Uncovering Iran's Mobile Legal Intercept System - The Citizen Lab

Motamedi, M. (2 October 2019) *Locked out: Why is Amazon blocking Iranians from its services?* Al Jazeera. Available at: [Online] https://www.aljazeera.com/economy/2019/10/2/locked-out-why-is-amazon-blocking-iranians-from-its-services

NPR (5 February 2023) *Iran acknowledges it has detained 'tens of thousands' in recent protests.* Available at: [Online] https://www.npr.org/2023/02/05/1154584532/iran-acknowledges-it-has-detained-tens-of-thousands-in-recent-protests

OONI (25 September 2022) *Iran blocks social media, app stores, and encrypted DNS amid Mahsa Amini protests*. Available at: [Online] https://ooni.org/post/2022-iran-blocks-social-media-mahsa-amini-protests/

RadioFreeEurope (9 September 2022) *Iran Accused of Secretly Implementing Controversial Draft Internet Bill*. Available at: [Online] https://www.rferl.org/a/iran-internet-bill-controversy-secretly-implementing/32026313.html

Rahimpour, R. (16 September 2022) *Fury in Iran as young woman dies following morality police arrest, BBC News Persian*. Available at: [Online] Fury in Iran as young woman dies following morality police arrest - BBC News

Reporters Without Borders (Last access 9 April 2024) *Index*. Available at: [Online] Iran. https://rsf.org/en/index

Saikal, Amin and Vestenskov, David. (2020) "Iran's National Security and Operational Capability", *Scandinavian Journal of Military Studies,* Vol 3, No 1.

Shakibi, L. (28 September 2022) *Government Use of AI-enabled Facial Recognition Systems*, FilterWatch. Available at: [Online] https://filter.watch/en/2022/09/28/policy-monitor-august-2022/

Syed, A. (22 November 2022) *Iran Has a Long History of Political Activism and Protest. Here's what to Know*, TIME. Available at: [Online] Iran's History of Protest and Activism: What to Know | Time

The Intercept (28 October 2022) *Iran's SIAM manual for tracking and controlling mobile phones*. Available at: [Online] Iran's SIAM Manual for Tracking and Controlling Mobile Phones - The Intercept

Zetter, K. (31 July 2020) *How cops can secretly track your phone*, The Intercept. Available at: [Online] https://theintercept.com/2020/07/31/protests-surveillance-stingrays-dirtboxes-phone-tracking/