

ARTICLE 19



Iran: Tightening the Net 2020

After Blood and Shutdowns.

First published by ARTICLE 19, September 2020

ARTICLE 19
Free Word Centre
60 Farringdon Road
London EC1R 3GA
United Kingdom
www.ARTICLE 19.org

Text and analysis Copyright ARTICLE 19, September 2020 (Creative Commons License 3.0)

Typesetting, Ana Z.

ARTICLE 19 works for a world where all people everywhere can freely express themselves and actively engage in public life without fear of discrimination. We do this by working on two interlocking freedoms, which set the foundation for all our work. The Freedom to Speak concerns everyone's right to express and disseminate opinions, ideas and information through any means, as well as to disagree from, and question power-holders. The Freedom to Know concerns the right to demand and receive information by power-holders for transparency good governance and sustainable development. When either of these freedoms comes under threat, by the failure of power-holders to adequately protect them, ARTICLE 19 speaks with one voice, through courts of law, through global and regional organisations, and through civil society wherever we are present.

About Creative Commons License 3.0: This work is provided under the Creative Commons Attribution-Non-Commercial-ShareAlike 2.5 license. You are free to copy, distribute and display this work and to make derivative works, provided you: 1) give credit to ARTICLE 19; 2) do not use this work for commercial purposes; 3) distribute any works derived from this publication under a license identical to this one. To access the full legal text of this license, please visit: <http://creativecommons.org/licenses/by-nc-sa/2.5/legalcode>

CONTENTS

Executive Summary	4
Acknowledgements	6
Glossary	7
Introduction	12
The big picture: Internet censorship in Iran	13
International Human Rights Standards on shutdowns	14
Chapter 1: The anatomy of the shutdown	15
Impact of the shutdown	17
A timeline	18
Chapter 2: The National Information Network and shutdowns	21
What is the NIN?	23
Users driven to local services	24
The role of US sanctions	25
Proposed bill could further nationalise infrastructure and data	27
Lack of transparency around shutdowns and the NIN	28
Chapter 3: Iran's Internet Infrastructure	30
ISPs, gateways, and shutdowns	31
The structure of connection in Iran	32
Two entities controlling international gateways: TIC and IPM	32
Decentralising access: changes since November 2019	34
Why decentralise?	34
ISPs enact government censorship	37
Chapter 4: Iran's Internet decisions	38
Ordering a shutdown	39
Power Structures Involved In Iran's Internet Decisions	40
Internet Policy: where does the power lie?	42
Changing the rules for ordering an Internet Shutdown?	44
Recommendations	45
Endnotes	54

1 EXECUTIVE SUMMARY

In November 2019, protests broke out across Iran over a fuel price hike; authorities responded with violence and repression. They also disconnected millions of Iranians from the Internet.

Iran's November shutdowns were unprecedented in length and reach. On a vast scale, they cut people off from vital information and from each other. Authorities subjected protesters to violent assaults without the exposure that access to the Internet enables.

The ability to conduct these shutdowns is the culmination of many policies, technological developments, and systems of centralised control that permeate Iran's system, and especially its Internet governance.

This report takes a close look at the Internet shutdowns that accompanied the protest period from 15 November to 27 November, as well as the mechanisms, infrastructure, law, and policies that enabled this kind of disconnection. It then looks at the aftermath of the protests and the outlook for Internet governance and connectivity in Iran.

INTRODUCTION

Here we provide the context to the November 2019 unrest and crackdown, as well as discussing the other forms of censorship used by the Iranian authorities to control the flow of information within Iran's borders. We also lay out international human rights standards on Internet shutdowns.

CHAPTER 1: THE ANATOMY OF THE SHUTDOWN

This chapter explains in detail the timeline of the shutdown, from the announcement of the price hikes that sparked nationwide protest to the reconnection later on. It also discusses the immediate effects of the shutdown and the consequences for protest and information during that time.

CHAPTER 2: THE NATIONAL INFORMATION NETWORK

Chapter 2 examines one of the key elements which enabled November's unprecedented shutdowns: the National Information Network (NIN).

Shutdowns generally result in severe financial losses, due to unavailable services and loss of communication with global partners and supply chains. Iran, however, has spent recent years building a NIN (a type of national Internet), which hosts a number of key services and government functions.

While access to the global Internet was cut off, domestic Internet services (hosted on the NIN), such as national banking, local applications, government websites and services, remained online. This minimised losses and kept the government functioning nearly as normal throughout the shutdown.

The chapter documents the development of the NIN and its role in Internet shutdowns, including the significance of US sanctions on its development and the digital rights of Iranian citizens.

It also looks at new bills that propose to entrench the NIN and pose various concerns for digital rights.

CHAPTER 3: IRAN'S INTERNET INFRASTRUCTURE

Iran's authorities have large-scale control over about 57.4 million Internet users in a total population of about 82 million. This requires a tight grip on both the national infrastructure and its Internet actors.

The chapter explains how the shutdown was carried out. Under orders of the National Security Council (NSC), the shutdown was carried out by Internet Service Providers (ISPs) and, during the protests, access to international gateways was entirely under government control.

This chapter also highlights that the connections infrastructure underpins the authorities' high level of control. It looks at the control of international gateways, and documents changes in the infrastructure, including the decentralisation of access to gateways. ISPs remain under strict control of the government.

CHAPTER 4: IRAN'S INTERNET DECISIONS

The shutdown was distributed to ISPs by the Communications Regulatory Authority, under the Ministry of Information and Communication Technology (ICT), ordered by the NSC.

This information alone, however, does not begin to tell us who and which factions of Iranian governance were behind November's events. This chapter attempts to explore further the accountability, or lack thereof, for the crackdown on both digital and protest rights.

Ambiguity about the processes of Internet decisions is a hallmark of the overall governance system in Iran. Although some members of President Rouhani's administration have apologised for the shutdowns, others, like Rouhani's Minister of Interior, have vehemently defended them. The government has not transparently documented what roles they played.

This chapter maps where power lies, and analyses recently proposed reforms to decision-making processes.

RECOMMENDATIONS

We end this report by making a series of recommendations to the Iranian authorities and international bodies to ensure the right to access the Internet and, in turn, freedom of expression in Iran.

2 ACKNOWLEDGEMENTS

ARTICLE 19 appreciates research inputs by Project Ainita to this report and contributions by researchers who wish to remain anonymous.

The ARTICLE 19 Middle East and North Africa (MENA) programme focuses on a number of countries in the region with concerns over their records on freedom of expression in the world. Many countries in the region lack legal protections for human rights and the rule of law is undermined by a lack of independent judiciaries. The 2011 Arab Spring popular protests brought hope for improvements, but devastating wars, foreign intervention, and instability have since made it an extremely dangerous environment for journalists, civil society, and human rights defenders, forcing millions to leave in search of safety. As war and conflict tear apart infrastructure and cause huge regression in development indicators across Yemen, Syria, Libya, and Iraq, elsewhere repressive governments in Saudi Arabia, Iran, Egypt, and Bahrain have reinforced anti-human rights practices, often in the name of national security and counterterrorism. ARTICLE 19's work on Iran focuses on monitoring laws, policies, and regulations that affect freedom of expression and information online and offline. We monitor Iran's complex Internet policies and respond to evolving threats online.

If you would like to discuss this report further, please contact Mahsa Alimardani at mahsa@ARTICLE 19.org

3 GLOSSARY

English	Acronym	Explanation
Autonomous System	AS	<p>The Internet is a network of networks broken up into hundreds of thousands of smaller networks known as autonomous systems (AS). Each of these networks is essentially a large pool of routers run by a single organisation. If we continue to think of Border Gateway Protocol (BGP) as the postal service of the Internet, ASs are like individual post office branches. A town may have hundreds of mailboxes, but the mail in those boxes must go through the local postal branch before being sent to another destination. The internal routers within an AS are like mailboxes: they forward their outbound transmissions to the AS, which then uses BGP routing to send these transmissions to their destinations. AS typically belong to ISPs, other tech companies, universities, government agencies, or scientific institutions. Each AS wishing to exchange routing information must have a registered autonomous system number (ASN). Internet Assigned Numbers Authority (IANA) assigns ASNs to Regional Internet Registries (RIR), which then assigns them to ISPs and networks. ASNs are 16-bit numbers between 1 and 65534 and 32-bit numbers between 131072 and 4294967294. As of 2018, there are approximately 64,000 ASNs in use worldwide. These ASNs are only required for external BGP.</p>

English	Acronym	Explanation
Border Gateway Protocol	BGP	BGP is the postal service of the Internet. When someone drops a letter into a mailbox, the postal service processes that piece of mail and chooses a fast, efficient route to deliver that letter to its recipient. Similarly, when someone submits data across the Internet, BGP is responsible for looking at all the available paths that data could travel and picking the best route, which usually means hopping between AS. BGP is one of the key protocols that make the Internet work. It does this by enabling data routing on the Internet. When a user in Singapore loads a website with origin servers in Argentina, BGP is the protocol that enables that communication to happen quickly and efficiently. [Source: Cloudflare]
Committee Charged with Determining Offensive Content	CCDOC	The CCDOC was established in 2009 as per the Computer Crimes Law that was ratified in the same year. It is a multi-agency oversight body that is in charge of online censorship in Iran.
Communications Regulatory Authority	CRA	Part of the Ministry of ICT, the CRA is responsible for regulating communication operators, including ISPs, mobile, and landline operators.
Computer Crimes Law	CCL	Introduced in 2009, the Computer Crimes Law is part of Iran's Islamic Penal Code.
Draft Data Protection Act or Personal Data Protection and Safeguarding Draft Act		A bill sponsored by the Ministry of ICT, which is purportedly designed to protect users' privacy. It is pending cabinet ratification before being sent to the parliament for review.
Fixed Communication Provider	FCP	A licence for private companies to become telecommunications entities (limited to Internet-related services).
Guardian Council of the Constitution (aka Guardian Council)	GC	The GC is an oversight body tightly controlled by the Supreme Leader. It interprets the Constitution of the Islamic Republic, supervises elections, approves candidates for elections, and ensures legislation passed by the parliament is "compatible with the criteria of Islam and the Constitution."
Institute for Research in Fundamental Sciences	IPM	The IPM is affiliated with the Ministry of Science, and is one of the two sole providers of Internet protocol (IP) communication infrastructure in Iran. IPM only offers services to academic institutions.

English	Acronym	Explanation
International Gateways		International gateways provide access to international terrestrial, submarine, and satellite systems. They manage incoming and outgoing international voice and data traffic. Considering that international gateways establish interconnections between domestic and international networks and determine the affordability and capabilities of broadband access, regulation of international gateways is an essential instrument in access to the international Internet. International gateways also play a critical role in addressing potential bottlenecks in data traffic that can have significant repercussions on downstream national markets.
Internet Service Providers	ISP	<p>An ISP is an organisation that provides services for accessing, using, or participating in the Internet. ISPs can be commercial, community-owned, non-profit, or otherwise privately owned.</p> <p>Services typically provided by ISPs include Internet access, Internet transit, domain name registration, web hosting, Usenet service, and colocation.</p> <p>An ISP typically serves as the access point or the gateway that provides a user access to everything available on the Internet.</p>
Iran Audiovisual Media Regulatory Authority	SATRA	SATRA, a regulatory arm of the state-run broadcaster IRIB, was established in September 2015 after Supreme Leader Ayatollah Ali Khamenei called on authorities to regulate cyberspace and content distribution on the Web.
Iranian Cyber Police	FATA	Iranian Cyber Police (aka FATA) is a unit of the Islamic Republic of Iran Police, founded in January 2011.
Islamic Republic of Iran Broadcasting	IRIB	IRIB is an Iranian state-controlled media corporation which holds a monopoly of domestic radio and television services in Iran. Supreme Leader Ayatollah Ali Khamenei appoints the IRIB's CEO.
Judicial System of Iran / Judiciary		The judiciary operates based on the Islamic Penal Code. It has different divisions dealing with civil, criminal, security, and cyber crimes. It has played an active role in banning online platforms and it is part of the decision-making process when it comes to Internet policy. Its chief is appointed by the Supreme Leader who has tight control over the judicial system.

English	Acronym	Explanation
Ministry of Information and Communications Technology of Iran	Ministry of ICT	The Ministry tasked with the portfolio related to all communications in Iran.
Ministry of Interior		The Ministry of Interior is in charge of performing, supervising, and reporting elections, policing, and several other security-related issues.
Mobile Telecommunication Company of Iran	MCI	MCI, which also operates under the brand name "Hamrahe Aval", is the largest mobile operator in Iran. According to the CRA, it has a 53.14% share of the market.
MTN-Irancell		MTN-Irancell is the second largest mobile operator in Iran, with a 43.45% share according to the CRA. Irancell has two shareholders: Iran Electronic Development Company (IEDC) (51%) and MTN Group Limited (49%). IEDC currently has two key shareholders: Mostazafan Foundation (controlled by the Supreme Leader Ayatollah Ali Khamenei) and Iran Electronics Industries (aka SAIRAN controlled by the Iran's Ministry of Defence).
National Information Network	NIN	There are a number of contesting meanings for this, but it ultimately refers to the hosting of data centres, servers, and related Internet infrastructures within the borders of Iran.
National Security Council	NSC	The NSC has been a subordinate subcommittee of the Supreme National Security Council (SNSC) since 1989. By law, it is led by the President's Minister of Interior and deals with domestic security and governance. In Persian, the main SNSC body is the "Shoraye Aali Amniat Melli" and the subgroup is called "Shoraye Amniat Keshvar". Melli means "nation" and Keshvar means country, but the real difference lies in the omission of "Supreme" from the subgroup.
Revolutionary Guards or the Islamic Revolutionary Guard Corps or the Islamic Revolution Guard Corps	IRGC	Iran's IRGC was founded in April 1979 after the Iranian Revolution by order of Ayatollah Ruhollah Khomeini. The IRGC was founded to defend the Islamic Republic's ideological system and to provide a counterweight to the regular armed forces. It has since become a major military, political, and economic force in Iran, with close ties to the Supreme Leader Ayatollah Ali Khamenei. The IRGC's chief and top commanders are appointed by the Supreme Leader.

English	Acronym	Explanation
Social Media Organisation Bill		The Social Media Organisation Bill is a bill that has been in the making since October 2018. A controversial clause in the initial draft of the bill would transfer control of Iran's Internet gateways from the civilian government to the Passive Defence Organization of Iran, which is controlled by the General Staff of the Armed Forces. The Iranian Parliament's Research Centre has recommended that the responsibility should be transferred to the SNSC. Both General Staff of the Armed Forces and the SNSC are controlled by the Supreme Leader Ayatollah Ali Khamenei.
Supreme Council of Cyberspace	SCC	The SCC was established by order of the Iranian Supreme Leader Ayatollah Ali Khamenei in March 2012. As stated in the SCC's charter, the body is tasked with developing the Islamic Republic's Internet policies.
Supreme National Security Council	SNSC	The SNSC, mandated by Article 176 of the Constitution of the Islamic Republic of Iran and created in 1989, is a security council presided over by the President and tightly controlled by the Supreme Leader. The council determines defence, national security, and foreign policies of the Islamic Republic.
Telecommunication Company of Iran	TCI	TCI is a semi-state-owned company with a strong monopoly over the landline telecom network. In addition to telephony services, it also sells broadband Internet services. It is also the parent company of Mobile Telecommunication Company of Iran (MCI) and holds 83.91% share in the mobile operator. IRGC-owned Mobin Trust Consortium is TCI's majority shareholder, with a 36.99% stake in the company, followed by the government, with 19.76%.
Telecommunication Infrastructure Company	TIC	TIC operates under the auspices of the Ministry of ICT. It is one of the two sole providers of IP communication infrastructure to all private and public operators in Iran.

4 INTRODUCTION

In November 2019, protests erupted in Iran over an increase in fuel price. The authorities responded with violence and repression, violating human rights guaranteed by international human rights law and the Iranian Constitution, including the right to assembly, freedom from inhuman and degrading treatment, right to life, and freedom of expression.

Unlawful and excessive force against protesters made it one of the bloodiest periods in Iran for the right to protest since the 1979 Revolution. The death toll ranges from verified reports of 304 to unconfirmed reports of up to 1,500 deaths. The number of those injured by security forces was estimated at 4,800.

During the protests, authorities also disconnected millions of Iranians from the Internet.

Intentional centralisation over the years has enabled Iran's Government to take the country offline, as happened in November. The ability to conduct these shutdowns was the culmination of many developments in Iran's Internet infrastructure, including the development of a National Information Network (NIN) and the centralised control which permeates the Islamic Republic of Iran's system. The United States and its sanctions regime have also played a detrimental role.

Protests beget Internet shutdowns in Iran. In recent years, this has become the reality for Iranians exercising the right to protest. Most frighteningly, as the days of the shutdown continued, authorities took advantage of the communications blackout to act with impunity.

It was nearly impossible to document the state's violence in real time. Access to the Internet and global data was cut off, while platforms that were still online – hosted domestically on the NIN – were closely monitored and controlled by authorities themselves. Shutting down the Internet gives authorities a certain amount of space to commit violent acts of repression without the news reaching citizens inside or outside of its borders, therefore avoiding further outrage.

It took months after the protests to gain verified documentation of the lives lost and proof that protesters and others were indiscriminately and unlawfully killed.¹

The lack of accountability for these violations of international human rights law remains a grave concern. There has still been no recognition by members of the Iranian Government or other state institutions that November's Internet shutdown is a violation of human rights.

Although some members of President Rouhani's Administration have denounced and apologised for the shutdowns, they have not transparently documented what roles they played within the decision-making bodies that ordered the shutdowns, of which they are prominent members.

ARTICLE 19 remains certain that there will be no space for Iranians to protest and exercise their freedom of expression, opinion, or assembly rights without the darkness of another Internet shutdown.

Sources (who wish to remain anonymous) speaking to ARTICLE 19 have said that, within internal meetings of the Iranian judiciary, officials have indicated that shutdowns can be triggered in the event of any unrest in the country.

These statements have proven true during recent protest outbreaks in July 2020. As protests broke out in the city of Behbahan on the evening of 16 July, the unrest quickly resulted in a shutdown of the Internet in that particular city until the early morning hours of 17 July.²

Indeed, lower profile events since November 2019 have shown once again the authorities' reliance on shutdowns and disruptions to repress demonstrations that criticise the state, including memorials for those killed during the protests throughout December³ and massive online protests against the execution sentences of three November protesters.⁴

THE BIG PICTURE: INTERNET CENSORSHIP IN IRAN

Iran's authorities have extensive control over around 57.4 million Internet users in a total population of about 82 million.⁵ This control has been achieved through extreme centralisation of both the infrastructure and authority over telecommunications companies and actors.

In addition to shutdowns, Internet censorship exists in many forms in Iran. Authorities routinely block or filter certain websites and applications; however, Iranians have ways to bypass this former technique through circumvention tools, which are used by a large subset of Iran's Internet users.

Websites for national newspapers, news agencies, or entities that exist within Iran constantly risk censorship, sanctions, or even closure by authorities. They therefore exercise a high degree of self-censorship, carefully conforming to what is acceptable to authorities.⁶ Iran's systems of censorship have a chilling effect on lawful speech, further tightening the realm of freedom of expression online and in the press.

The demonstrations of the 2009 Green Movement⁷ saw Iran's first nationwide shutdown, along with the subsequent censorship of social media platforms such as Twitter and Facebook.⁸ This seminal event realigned much of Iran's national security focus and resources towards Internet governance, policies, and laws.⁹

The events of 2009 led to the establishment of institutional and legal mechanisms for regulating the Internet: the Computer Crimes Law (CCL), the establishment of the Supreme Council of Cyberspace (SCC), and the prioritisation of the development of the NIN, a nationalised Internet which, until then, had only been an idea within government.¹⁰

Throttling Internet connectivity – or deliberately reducing Internet speeds – is another form of Internet censorship the government has administered, as illustrated during the 2013 presidential elections.¹¹ This throttling made Internet usage excruciating and rendered the use of virtual private networks useless.¹² These were intentional tactics to hinder access to the Internet and, in turn, tighten the space for freedom of expression during a time the government considered sensitive and ripe for political mobilisation or protest.

Nationwide protests from December 2017 to January 2018 were another key moment for Iran's Internet policy as shutdowns became increasingly interwoven with the National Internet Project.¹³

Internet shutdown techniques are the bluntest form of censorship, and as compared to the techniques described above, they increase the government's ability to control access to the Internet. A complete Internet shutdown does, however, incur many costs for the government, including severely impacting the country's essential services and economy.

This is why domestic Internet services remained online, but access to foreign Internet services and websites was cut off during the nationwide protests on 15 November 2019. National banking, local applications, and government websites and services hosted on the NIN were available. The NIN makes shutdowns convenient for authorities because it keeps essential services and tools online, even amid a shutdown.

INTERNATIONAL HUMAN RIGHTS STANDARDS ON SHUTDOWNS

Iran's Internet shutdowns violate a number of international human rights standards.

The United Nations Human Rights Council Resolution 32/13, adopted by consensus in June 2016, "condemns unequivocally measures to intentionally prevent or disrupt information online in violation of international human rights law" and called on states to desist from such practices.¹⁴

In its General Comment No. 34 of 12 September 2011, the UN Human Rights Committee considers that the generic bans on the operation of certain Internet sites is incompatible with Article 19(3) of the International Covenant on Civil and Political Rights (ICCPR). Indeed, the General Comment states:

“*Any restrictions on the operation of websites, blogs or any other Internet-based, electronic or other such information dissemination system, including systems to support such communication, such as Internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3 [of Article 19].*

“ Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3. It is also inconsistent with paragraph 3 to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government.”¹⁵

Additionally, at the end of November 2019, several UN Special Rapporteurs released a statement expressing “grave concern” over the disconnections.¹⁶

However, the Iranian state authorities erroneously reinterpret their human rights obligations. The Minister of Information and Communications Technology (ICT) has indicated that authorities have a right to enact shutdowns, through their membership and adherence to the regulations of the International Telecommunication Union (ITU):

“ The International Telecommunications Union, which we are attached to, in their constitution's Article 34, second line, accept this as law, however this law is in need of clear transparent procedures, especially so businesses and entrepreneurs are aware of what such emergencies are.”¹⁷

The ITU Constitution does leave room for countries to justify shutdowns, which is fundamentally at odds with the human rights norms outlined above. Article 34 and 35 of the ITU Constitution gives states the right to cut off access to telecommunication services or “international telecommunication services” if they prove “dangerous to the security of the State.”¹⁸

Regardless of the ITU Constitution, states must be held accountable for their human rights violations. The values set out in the ITU’s own strategic plan include a recognition of the “overarching pre-eminence of human rights,” including the rights to freedom of expression and privacy.¹⁹ At the same time, the ITU Constitution requires any member states, including Iran, who undertake the “stoppage of telecommunication,” such as an Internet shutdown, to meet certain criteria, which includes informing the ITU and other members about the action.²⁰ This is a minimum requirement for transparency and accountability, which Iran has failed to follow.

Chapter 1: The anatomy of the shutdown



IMPACT OF THE SHUTDOWN

At midnight on 15 November 2019, the Iranian Government surprised the nation by implementing new fuel rations and increasing the price by 50% for rationed fuel and 300% for free market fuel.

This sparked almost immediate national social unrest and a heavy-handed response from Iran's armed security forces. The first night of protests saw at least six deaths of protesters at the hands of Iranian authorities.²¹

Between Saturday 16 November and Thursday 21 November 2019, a nationwide Internet shutdown only enabled 4–7% connectivity.²² Most Internet connections to the global Internet on Iran's mobile carriers did not come back on until Wednesday 27 November.

It is important to note that many government officials argue that a "shutdown" never occurred because of the access to services on the domestic network of the NIN.²³ Despite the availability of access to NIN services, ARTICLE 19 recognises the loss of access to the global Internet as an Internet shutdown.

Iran implemented this shutdown with the cooperation of Iran's various Internet Service Providers (ISPs). ISPs received a notice from Iran's Communication Regulatory Authority (CRA), the regulatory body responsible for executing censorship and other Internet policies in Iran under the auspices of the Ministry of ICT. Such national security orders are mandatory and never challenged by ISPs, as mandated by Iran's vague national security laws.

It is not a coincidence that access to most of the Internet was lost as state violence started to increase. These disconnections meant three things:

1. Mobilisation for protests became severely limited because the type of communication that was occurring across Waze (the crowdsourced navigation application), messenger applications, and social media was banned. It could also lead to direct persecution if noticed on controlled services on the NIN, which are monitored by authorities.
2. The violence could not be properly documented or the documentation shared. This, therefore, could not inspire outrage or action from national and international audiences. Viral images of state violence, such as 2009's video of the killing of the peaceful protester Neda Agha Soltan, have massive symbolic power to affect hearts and minds inside and outside the country.²⁴
3. It became easy for the state authorities to manipulate the narrative of what was happening around the protests and explain violence without incriminating the state, especially as the Internet shutdown was implemented alongside intermittent satellite TV jamming.²⁵

A TIMELINE

16 NOVEMBER 2019



Figure 1: A user on an MCI data plan loses mobile connectivity at 15:00 on the first day of protests in Tehran.

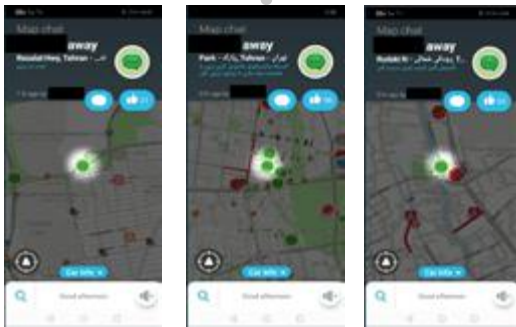


Figure 2: Screen captures from Tehran-based Waze users sharing information on where to park cars for protests on the afternoon of 16 November.

- In the early hours of 16 November 2019, the first reports began to arrive that the Internet had been cut off in cities like Ahvaz in southwest Iran, where protests had been most pronounced.²⁶
- Semi-state-owned MCI and Irancell, the largest mobile operators in the country, disconnected their cellular data connectivity on 16 November in an unprecedented move (Figure 1). Soon ISPs would disconnect home broadband connections.
- Immediately before the Internet was shut off in Tehran, reports from the city indicated increasing protest mobilisation.
- Users started organising meeting points for street protests on Waze, the crowdsourced navigation application, and social media platforms like WhatsApp, Telegram, and Twitter.
- The first screen capture in Figure 2 shows a user sharing their location for protesting and writing "screw the regime."
- The second screen capture shows a user indicating his location in the middle of the street and writing "wild things, turn off your cars and go play in the snow with your families until they bring the price back down."
- The third screen capture shows a user indicating to "turn off [cars] so they bring down the price."



Figure 3: Google Maps image of traffic jams caused by protests on 16 November.

- Google Maps (Figure 3) illustrates the scale of demonstrations. Traffic jams, caused mostly by parked-car protests, reached almost all major highways and streets, locking down most road traffic.

17 NOVEMBER 2019



Figure 4: The impact on the network from Oracle's Internet Intelligence data.²⁸

- Amnesty documented 100 deaths on 16 November.²⁷

- Disconnections occurred across the majority of Iran's ISPs, cutting off most links by 17 November around 14:00 (Figure 4).

- Amnesty documented 78 deaths on 17 November.²⁹

18-24 NOVEMBER 2019

- The Internet remained disconnected across the entire country for the next six days, and for longer in parts where unrest did not subside for the next 10 days.
- Many platforms and government services that operate or are available through the NIN remained online. Despite some initial technical glitches, most of these NIN services were working throughout the shutdown.

20 NOVEMBER 2019



Figure 5: SMS with instructions on reconnecting the country (see translation on page 21).*

- Snapp's Uber-like app, online taxi app, Tap30, and local navigation and messaging apps, such as Balad and Soroush messenger, were offered through the NIN and were accessible.

- However, there were some gaps, for example Iran does not have a functional domestic search engine (see Chapter 2). In a hasty move, ISPs launched a directory website of all domestic services and sent SMS messages to some mobile users to inform them of this directory.

- ISPs (see Chapter 3) received a notice from the CRA to start phasing in reconnections.

- Figure 5 shows an SMS message sent to an Iranian ISP on instructions on how to reconnect the country (source wishes to remain anonymous). The source indicated that other ISPs received the same instructions.

1. *The economic need to reconnect to the global Internet.* The notice described these “economic priority” organisations as “companies, service offices, businesses, universities, research organisations, religious organisations, government offices, police forces, start-ups news agencies, newspapers and needed websites.”

2. *Was the area being reconnected within one of the zones of unrest.* Zones of unrest included Shiraz city, Khuzestan Province, Alborz Province, and cities west of Tehran.

- Khuzestan, Sistan, and Balochistan Provinces only came back online a couple weeks after the rest of the country because protests continued in these regions.³⁰

25 NOVEMBER 2019



Figure 6: Iran's ISPs resume majority connectivity by 25 November 2019 (from RIPE STAT).

- ISPs started to appear online again (Figure 6).

27 NOVEMBER 2019

- All ISPs were back online, operating and reconnecting Iranian users to international Internet services.

✳ A text message sent to an employee of an ISP provider about the different “phases” of reconnection. Translation of the text: “Hello, These are the guidelines you need to read. Phase 1 of Internet reconnections: Operators can connect users which are 1 of the following categories to the Internet: companies, service offices, businesses, universities, research organisations, religious organisations, government offices, police forces, start-ups news agencies, newspapers and needed websites (excluding users in Shiraz city, Khuzestan province, Alborz province, cities in west of Tehran) [There is some ambiguity over who sent these notices. In normal times TIC handles issues related to online censorship. The CRA may have transmitted orders to ISPs during Nov protests.]. They should use static IP address ranges and they should announce their IP addresses to the centre for network security. Important note from technical implementation perspective: they should only whitelist allowed cities w/ static IP range and remove the nonallowed cities with static IP range and remove the non-allowed cities from the whitelist. For example, Tabriz university has permission to connect but Ahwaz university doesn't have the permission. To clarify home users with or without static IPs don't have the permission to connect. Important note: due to the fact that higher level operators can't determine downstream operator's user use cases, they can whitelist all the static IP ranges of the downstream ISP with a contract in place that they will apply the right policy.”

Chapter 2: The National Information Network and shutdowns



Iran is not the only country that imposes Internet shutdowns. The length and scale of the November shutdowns have been outmatched by the July 2020 Ethiopian shutdowns, as well as continuous disconnections in parts of Myanmar. Both Myanmar's and Ethiopia's shutdowns were longer than Iran's, but Ethiopia's affected a larger population.³¹

However, Iran is unique in implementing a backup system of connection through the NIN. Iran's development of the NIN,³² which was prioritised by governments following the 2009 protests, has been one of the reasons why nationwide shutdowns have become an effective tool to suppress protest.

Shutdowns are generally costly for countries, resulting in losses that can be equivalent to millions of US dollars due to services that are no longer accessible or the loss of communication with global partners and supply chains.³³ Shutdowns become less expensive for Iran, however, as more services become reliant on the national infrastructure hosted on the NIN.³⁴

Protests in December 2017 and January 2018 triggered some of Iran's first shutdowns, but even then there was assurance that core government and financial services in Iran would remain online on the NIN. This pattern looks to continue, and even deepen, as increased reliance on the NIN is fostered among services and users.

WHAT IS THE NIN?

In 2012, Iran initiated the development of a NIN, a domestic Internet infrastructure hosted inside Iran, with the aim of being secure from foreign attacks, but may potentially be disconnected from the global Internet.

Elements of the NIN have already been launched, including national infrastructure for banking and payment methods. The existence of the NIN has not yet resulted in long-term disconnection from the global Internet, but it has been a short-term tool to support shutdowns during protests and unrest.

The NIN allows authorities to monitor content based on political, cultural, and religious criteria. This bolsters current violations of freedom of expression and access to information inherent in Iran's system of controls. Furthermore, the monitoring and oversight of data and traffic on this network undermines data protection and the right to privacy for Iranian users.

Concerns about the long-term aspirations of this project have grown in recent years due to increasing efforts by the authorities to drive Internet users in Iran towards domestic platforms, while reducing access to and reliance on content and services available through the global Internet.

In January 2019, the government announced a planned "experiment in disconnecting the Internet" designed to test the robustness of its domestic financial payment infrastructure. However, the experiment was called off in response to widespread opposition.

In May 2019, the Minister of ICT noted: “We are preparing for scenarios where the global Internet will be cut off [by the US].”³⁵ Sources within the US Government have repeatedly denied they would “cut off” Iran by preventing companies that provide international terrestrial or submarine networks from enabling international connections with Iranian ISPs.

ISPs are already required to cooperate and hand over data to government authorities, especially to institutions known for conducting monitoring and surveillance, such as the Ministry of Intelligence, Iran’s Cyber Police (FATA), and the Islamic Revolutionary Guard Corps (IRGC) – including their particular cyber institutions Gerdab and/or their security arms, IRGC Intelligence Organization and IRGC Intelligence Protection Organization.

The NIN will bolster the capabilities of repressive institutions if users become reliant on their services for all aspects of their day-to-day lives. Institutions like the IRGC are widely known to partake in monitoring projects and surveilling telephone calls, social media accounts, and hacking into emails to persecute activists, journalists, and human rights defenders.

These concerns have been further exacerbated by new bills on data protection and social media that will create legal frameworks to further control and monitor Internet data, as well as placing content and services in the hands of regulators and authorities, and onto the NIN.

USERS DRIVEN TO LOCAL SERVICES

Strengthening local platforms and driving local users towards them is central to the NIN strategy. This has included efforts to undermine net neutrality by allowing and, in some instances, ordering ISPs to subsidise the use of domestic platforms.³⁶

Ultimately, pushing users to use domestic services strengthens the government’s control over content, surveillance, and monitoring capabilities, and raises concerns for the protection of the right to privacy and freedom of expression.

That push is not an easy one, however. Despite state subsidies and massive publicity and effort to bring users of encrypted messenger Telegram to the Islamic Republic of Iran Broadcasting (IRIB)-developed Soroush messenger, this has been a failed project.³⁷ Although Telegram has been banned in Iran, users have largely remained on Telegram, and partially migrated to WhatsApp. All statistics show that foreign platforms are Iran’s most used messenger applications.³⁸

Several “domestic” search engines have been launched in Iran, especially during the administration of Mahmoud Ahmadinejad. However, these services typically use Google Search to find results and then display them according to the content regulations in Iran.³⁹ Most of these services crashed during the shutdowns.⁴⁰

Video-sharing application Aparat is one of the few national platforms that has succeeded, due to a strong boost by subsidised domestic video streaming costs and the cost of using mobile data on foreign video streaming.⁴¹

Previous localisation efforts have included state incentives for Iranian software developers to build messaging applications to rival foreign ones. Developers have been rewarded on the basis of their numbers of users.⁴²

There have also been institutional requirements to follow updates about university programmes or government departments that communicate privately or publicly through national messengers such as the IRIB's messenger Soroush.⁴³ However, most flout this rule, including members of the Ministry of ICT who are well known to communicate with associates and journalists through Telegram.⁴⁴

During the Internet shutdown, many users reported an increase in the advertising for Iran's version of Waze, called Balad. The Iranian app works with similar crowdsourced reporting features as Waze, but is hosted on the NIN and subject to government oversight and monitoring. The advertisements took advantage of the nature of the shutdowns and the ongoing availability of platforms on the NIN, and emphasised that Waze was offline but Balad was working.⁴⁵

THE ROLE OF US SANCTIONS

Limits on online expression, and privacy more generally, have been exacerbated by the impact of a decade of sanctions against Iran. Imposition of sanctions by the US is also among the reasons given for the launch and development of the NIN.⁴⁶ The problems that sanctions have created are three-fold. First, they create severe limitations in terms of services Iranians can access. Second, they provide additional excuses for the government to tighten and centralise control over the Internet under unmerited fears the US "will cut all access to the global Internet" because of sanctions; and third, the economic isolation caused by sanctions incentivises authorities to further isolate the Internet.

Sanctions have impelled Iranian authorities to develop an Internet infrastructure that is neither reliant on nor vulnerable to the predominantly US technical foundations and ownership of the global Internet. Although this US-based ownership is tied to private industry and not directly the US Government, these US companies are prevented from providing services within Iran because of US Government sanctions.

Iranian officials express concern that Iran could be disconnected from the global Internet at infrastructural level (global land and submarine cables) by the US. Although this is a claim denied by US Government officials,⁴⁷ it has been used as a justification to continue to strengthen and expand the NIN by Iranian officials, such as Minister of ICT Azari Jahromi.⁴⁸ In May 2019, Jahromi announced the creation of a working group to discuss different scenarios and strategies to counter US sanctions that block Iranians from key Internet infrastructure.⁴⁹

In March 2010, the Ministry of ICT declared that all public organisations or legal entities⁵⁰ should relocate their websites to domestic hosts within six months, although the process to migrate websites was already underway because of sanctions. Information technology and hosting services for “.ir” domains were included in the US sanctions against Iran, which led US companies to discontinue their hosting services for “.ir” websites before this policy.⁵¹ This meant that not only public organisations had to have national hosting, but because of US sanctions, any URL containing an “.ir” domain would now turn to national alternatives.⁵² US sanctions indirectly provide the groundwork and ammunition for increased implementation of the NIN, partly as a result of necessity and partly by playing into Iranian governmental propaganda regarding vulnerability to outside forces, justifying intensification for NIN implementation.⁵³ Sanctions are thus helping with the overall project of undermining access to a free Internet and, as a result, freedom of expression.

Government blocking and filtering can be circumvented by the use of technical tools, which many Iranians do use. However, many of these tools are hosted on services such as Github, Amazon Cloud, and Google Cloud, which are not accessible due to sanctions.

For example, DigitalOcean and Amazon Web Services (AWS), two major US cloud infrastructure providers, are blocked in Iran because of sanctions, meaning that Lantern, a circumvention tool that relies on those infrastructures, have been temporarily blocked in the past.⁵⁴

Limited access to these services forces an increased reliance on unsafe hosting and circumvention tools, which compromise users' data and security and result in developers relying on national services and infrastructures hosted on the NIN.

The potential for the US to cut off Iran's access to the global Internet is disputed and unclear, even according to the Iranian Government's own rhetoric. Jahromi's May 2019 comments about the possibility of the US sanctioning the global Internet were in stark contrast with his stance a year earlier, when he publicly contested the claims of Brigadier General Gholamreza Jalali (head of the Passive Defence Organisation of Iran) that: “The US can shut down Iran's Internet.”⁵⁵

In response, Jahromi said, “Access to the Internet is not controlled by anyone.⁵⁶ You can't say that the US controls the Internet and can cut Iran off.” His comments were echoed by his deputy Amir Nazemi who argued: “The US sanctioning the Internet” would be a far-fetched scenario.⁵⁷

The shift in Jahromi's rhetoric highlights a historic pattern. Some factions of the establishment have disposed of their more moderate stances in response to tightened sanctions and increased isolation of Iran from the global community.

The Minister has also cited the policies of Apple and Google to partially block Iranians from their services as a reason to further bolster the NIN. In March 2018, Apple made the decision to completely block access to its App Store in Iran⁵⁸. Access to the App Store was later restored for iOS users.⁵⁹

Furthermore, in March 2019 Apple started removing applications associated with developers in Iran. Google had already blocked its App Engine and other services on its Cloud Platform to users in Iran⁶⁰ and AWS has blocked parts of its services that it fears infringes on business or financial transactions from Iran.⁶¹

The aim of punishing Iran through economic isolation using sanctions is having repercussions on online freedoms. ARTICLE 19 believes the correlation between international trade and Internet freedom is clearer than ever: the NIN is successful in reducing costs to shutdowns only if businesses and transactions do not use foreign platforms and cooperation. Iran's economic isolation therefore reduces the costs of shutdowns and encourages further Internet isolation, as well as using Internet shutdowns as a tool of repression.

In addition, because so many businesses, start-ups, and corporations rely on communication and trade with international partners, the government and the people still experienced losses during the shutdown, despite the connections and platforms of the NIN.⁶²

Although priority for reconnection was given to business and entities that contributed to the economy, serious economic losses had already been sustained (see Chapter 1). Several officials within the Ministry of ICT published op-eds in local outlets, highlighting the economic impact of the shutdown and advocating the creation of a white list to curtail any impact of possible future shutdowns on businesses.⁶³

PROPOSED BILL COULD FURTHER NATIONALISE INFRASTRUCTURE AND DATA

Proposed and existing laws in Iran threaten to limit connectivity even further. Localisation of data, content, and Internet traffic to domestic platforms will have a detrimental effect on the diversity of content available online in Iran, as well as on the rights to freedom of expression and privacy.

Data localisation laws have been used in a number of jurisdictions as a pretext to limit access to social media platforms and attempt to control the data of users in their territories. In Russia, they have used data localisation to censor non-complying platforms such as LinkedIn and impose fines on others such as Twitter and Facebook.⁶⁴ In the US, national security concerns over Chinese-owned social media companies has also become a question for data localisation.⁶⁵

Forced data localisation makes it easier for authorities to access private communications. This is concerning in a country such as Iran where laws threaten privacy and the protection of individuals online. The processing of user data is undermined by the oversight powers given to authorities and the development of local applications without privacy protections (encryption is illegal according to Article 10 of Iran's CCL).

The "Preservation and Protection of Personal Data Bill" was introduced in July 2018. It reflects policies released by the SCC in 2017, which had the explicit aim of nationalising Internet infrastructure in Iran.⁶⁶

In May 2018, the Minister of ICT, Azari Jahromi, announced that his ministry welcomed the EU's General Data Protection Regulation (GDPR).⁶⁷ He promised to launch a data protection bill for Iran and engage in "constructive talks with the EU about mutual legal and technical assistance."

The Bill purports to protect the rights of individuals to have their personal data protected, but instead it is likely to enable further surveillance and censorship, reducing the availability of foreign-owned apps and social media platforms. It will thus increase reliance on less secure Iranian technologies hosted on the NIN.⁶⁸ The Bill applies to both private and public bodies, including the government, when they are collecting and processing personal data.

The current text is weak in many respects. For example, there is a total lack of data protection principles, including unclear material and territorial scope, a lack of an exemption for processing in the context of journalistic activity, weak access rights for the data subject, and a non-independent Data Protection Commission.

The most concerning part of the Bill is Article 34, which states that all social media and Internet services must store their data in Iran or foreign data centres approved by Iran (or be subject to blocking). Data localisation is a big step towards a national Internet infrastructure.

LACK OF TRANSPARENCY AROUND SHUTDOWNS AND THE NIN

Following the shutdowns, Iranian authorities made various statements about the role of the NIN in the shutdowns. Confusion remains over many of these statements, which seem to contradict one another. None of the statements admit responsibility or create space for accountability in relation to the shutdown.

At the end of November, UN Special Rapporteurs released a statement expressing "grave concern" about Iran's Internet shutdowns.⁶⁹

The spokesperson for Iran's High Council for Human Rights responded by claiming no such infringement on access to the Internet or freedom of expression had occurred, because every Iranian had access to the NIN, which contains communication and information.⁷⁰ Iran's High Council is part of the judicial system, generally a hard-liner institution, which is behind many of the existing policies and legal notices for censorship.

This position is at odds with how the Rouhani government has framed the issue. Both President Rouhani and Minister of ICT Jahromi have claimed that their active development of the NIN throughout this administration has not meant an intention to disconnect entirely from the global Internet.

The Minister of ICT recognised the disconnections from the global Internet as a shutdown, which contradicted the stance of Iran's High Council for Human Rights. The Minister of ICT has even gone as far as to personally apologise to Iranians for the disconnections, while assuring that the development of the NIN does not mean Internet shutdowns.⁷¹

In December 2019, Rouhani addressed parliament, declaring: "the National Information Network will be strengthened so people will not need foreign networks to meet their needs."⁷² Given Iran's lack of success in migrating Iranians to national alternatives from foreign platforms, this was seen as a declaration of potential enforcement measures and as "shutting" down access to foreign platforms.

Rouhani's Communications Deputy later clarified:

“ Speaking about the expansion of the National Information Network and independence in cyberspace does not mean shutting down the Internet and living in the Stone Age. The two (NIN and Internet) are complementary. Saying we must cut connections with the [outside] world is a sign of inability to understand life in a world of networks.”⁷³

In the current framework, the Supreme National Security Council (SNSC) or its subsidiaries order shutdowns. The Minister of ICT and his deputies have suggested that shutdowns should only be implemented after a parliamentary vote, as opposed to the arbitrary decision of the SNSC.⁷⁴

The Ministry officials declared they were writing a bill for these changes, but there has been no update since December 2019. The proposed idea for such a bill has given rise to severe concerns about the normalisation of states giving themselves the option to "shutdown" the Internet (see Chapter 4).

Chapter 3: Iran's Internet infrastructure



In this chapter, we try to understand the system of Iran's Internet infrastructure of control that enables complete authority to implement a shutdown. Despite popular opinion that an off switch existed to shut down the international Internet connection, the government maintained some connections while the rest of the country was shut down. In this section, we delve into the system of control that was built during the November 2019 shutdown, and has since evolved. Despite a move towards some infrastructural decentralisation, the system of control remains intact. We consider the potential positive outcomes for moves to privatise and decentralise more of the country's Internet infrastructure. However, ARTICLE 19 believes that the regulatory mechanisms in place (see Chapter 4) will mean these positive outcomes are impossible.

ISPs, GATEWAYS, AND SHUTDOWNS

International gateways provide access to international terrestrial, submarine, and satellite systems, and they also manage incoming and outgoing international voice and data traffic.

Without international gateways, the Iranian network cannot access the services of the global Internet. International gateways, however, are not required to access services on the NIN.

At the time of the shutdowns, all Iran's ISPs were connected to five international gateways, operating through two entities. These gateways were run by the Institute for Research, and Fundamental Sciences (IPM) as part of the Ministry of Science, Research, and Technology, and also the Telecommunication Infrastructure Company (TIC), which sits under the Ministry of ICT, and oversees IP communication infrastructure across the country.

Access to the global Internet was centralised to two government-controlled gateways. The two gateways (in November 2019) were the only access points for all international traffic and IP capacity and connectivity services in the country.

The UN Economic and Social Commission for Asia and the Pacific defined Iran's system of operating its international gateways as a "government monopoly"; most countries operate access to the gateways via open competition among private companies.

Despite this centralisation, the shutdown was not carried out by shutting down the gateways themselves. Instead, and to avoid destructive and costly disconnection, individual ISPs, who are beholden to the central government, were ordered to shut down. In other words, despite having the ability to use an 'off switch' to cut off international traffic, the government opted to systematically exercise their authority over multiple ISPs.

Disconnection and reconnection of ISPs were determined at the top level by the National Security Council (NSC), which is a branch of the SNSC, down through to the Ministry of ICT. Some ambiguity has been created by the Ministry of ICT

who has indicated the order went straight from the NSC to the ISPs, without the Ministry's involvement. Although officials publicly declared the NSC responsible, it cannot be independently confirmed that the order was not issued by the SNSC itself (see Chapter 4).

THE STRUCTURE OF CONNECTION IN IRAN

The majority of connections on the map for Iran's infrastructure during the shutdowns are domestic ISPs, which connect homes, mobile networks, and institutions to domestic and international networks. This is the first layer of providers that are connected directly to the international gateways (see Figure A1.1 in Annex 1).

There were five gateways interconnecting, or peering, to privately owned international transit providers, which are foreign companies providing international connectivity from the exterior to Iran's national network. A second layer of smaller ISPs connect the first layer of providers (see Figure A1.1 in Annex 1).

TWO ENTITIES CONTROLLING INTERNATIONAL GATEWAYS: TIC AND IPM

The IPM International Gateway, which provides access to the global Internet for research and educational institutes, largely stayed online throughout the November 2019 shutdown, or experienced shorter or intermittent periods of disconnection.⁷⁵

Internet users normally connect to the Internet through ISPs, which are then connected through the TIC Gateway. Although the notice sent to an ISP in Figure 5 is an example of notices sent to ISPs connected through the TIC gateway, the IPM gateway was regulated mainly through the institute's own systems.

Testimonies from university faculties and students attest to a wide variety of experiences of access and disconnection (Figure 7). For example, students at Shahid Beheshti reported regular access to the Internet, except for a period of minor disruption during the national shutdown.

The University of Tehran's dormitories only had their Internet cut off a few days into the nationwide shutdown, while students at Sharif University reported their Internet connections were cut off the same day as the nationwide shutdowns were imposed. Many students at the University of Tehran believe that their (much more) active and vocal student body was the reason they were kept online because university authorities feared protests or unrest.

Access to the Internet for these two universities was largely reinstated on 21 November, four days before the majority of the country started to come back online.








University	Disconnected 	Reconnected 
<p>Kerman University of Medical Sciences</p> 	<p>Connections cut on 15 November</p>	<p>23 November</p>
<p>Isfahan University of Technology</p> 	<p>Connections cut on 15 November</p>	<p>21 November</p>
<p>Shahid Bahonar University of Kerman</p> 	<p>Connections cut on 15 November</p>	<p>25 November</p>
<p>Shahid Beheshti University (Tehran)</p> 	<p>Never disconnected. Instagram and Telegram connected throughout the shutdown. Students only experienced a decline in the quality of services.</p>	
<p>Shiraz University of Technology</p> 	<p>Disruptions, but certain proxies were connecting students to all international services.</p>	

Figure 7: Disconnections and interruptions at various Iranian universities.

DECENTRALISING ACCESS: CHANGES SINCE NOVEMBER 2019

The centralised infrastructure that existed in November no longer exists. ISPs no longer rely on the two government-controlled Internet gateways, TIC and IPM. They now have the option to connect directly or via other intermediaries that are not owned by the state (Figure A1.2).⁷⁶

The decentralisation of the Iranian network's access to the global Internet means that different interest groups can play a role in developing and controlling Iran's communication infrastructure, while gaining access to the market and user data. Although these new stakeholders are not having an immediate impact on the nature of Internet policy and censorship mechanisms, they will be carving out a space for themselves for policy considerations in the future.

The smaller nodes in Figure A1.3 in Annex 1 are companies that have recently managed to establish international connections directly from their own networks. Permits for ISPs or organisations (Iranian AS) to directly connect with foreign-owned terrestrial, submarine, or satellite connections at the IP level (where the physical connection of the cables are still administered by the TIC) are a recent government decision, along with an increase in direct foreign connections and gateways.

These connections were not permitted in the past, and there has been no direct announcement of the change or explicit government policy shift in allowing these permits. Business insiders and technology journalists in Iran to whom ARTICLE 19 spoke had no insight into this policy shift.

WHY DECENTRALISE?

Although the system of decision-making and authority is still centralised, and censorship mechanisms remain extremely strong, this infrastructure-level decentralisation means more stakeholders are involved in the process of Internet administration. The breakdown of Iran's monopoly over telecommunications was not made with freedom of expression in mind, nor has the decentralisation led to immediate improvements for online freedoms.

However, creating more stakeholders through the existence of new private telecommunication entities, who rely on the Internet not being disrupted or shut down, is an important move in ensuring there are vested interests to prevent further shutdowns. The economic incentives in maintaining these international connections are vast and profitable for the national economy.

There are three probable reasons for this move towards decentralisation of access to Internet gateways:

1. It may be a response to US financial sanctions, which make it difficult for government entities to buy connectivity capacity from international companies

serving at gateways. International companies that run the terrestrial, submarine, or satellite connections that connect to the international Internet may have difficulty or are reluctant to create new contracts with Iranian companies. Since these private ISPs or other network operators are not directly state-owned, they have more flexibility for international contracts and payments.

2. This shift may be occurring because the former level of centralisation was unsustainable, and the TIC and IPM simply did not have the capacity to run and oversee all the nation's gateways.
3. It may be part of a strategy by the Ministry of ICT to break monopolies in Iran's communications market, including the monopoly held by the Telecommunication Company of Iran (TCI) (see below).

BREAKING TCI'S MONOPOLY

The TCI should be distinguished from the TIC. The TIC, which is controlled by the Ministry of ICT, establishes and regulates the communication infrastructure, whereas TCI is a semi-state-owned communication operator with an unchallenged monopoly over landline services, as well as selling broadband services and offering mobile connectivity through its subsidiary MCI (see Glossary).

Addressing the Iranian Parliament in June 2020, Minister of ICT Azari Jahromi blamed the TCI's monopoly on landline communications for disruptions in communication services following the Covid-19 outbreak and a surge in unmet demand for services.⁷⁷ He also explained the need for private companies to be allowed to play a more active role in expanding and employing the communication infrastructure.

This was echoed by his deputy Hamid Fatahi, who also serves as head of the TIC. Fatahi blamed the TCI for "disruptions in Internet services." He claimed that the government-controlled TCI "has no control" over some Internet service disruptions and that the TCI's monopoly had disrupted expansion plans.⁷⁸

Despite a CRA mandate for the TCI to share its network infrastructure with local ISPs⁷⁹ and Jahromi's announcement that they had agreed to do so (meaning that all private ISPs would be able to offer services through TCI's fibre-optic network),⁸⁰ the TCI is still the sole provider of landline Internet services in many areas in Iran.

Since 2017 – the beginning of Jahromi's tenure as Minister of ICT – the Ministry has been pushing for network decentralisation, not merely for access to gateways but also for opportunities for smaller and private companies to offer communication services, in addition to making the direct international connections (or "peerings" in technical terms).⁸¹

The Ministry of ICT has also encouraged ISPs to merge. Jahromi argues, "Mergers and acquisitions between local ISPs will enable private businesses to cut costs, raise funds, and compete with TCI." Jahromi has suggested that the CRA provides incentives; however, it is not clear what they might be. In 2017, and during Jahromi's tenure, HiWeb acquired Pars Online in a move promoted under this policy.⁸²

The merging of ISPs constitutes a major departure from the type of centralisation seen in November 2019. Some of these new international connections are through major private ISPs in Iran, which hold a Fixed Communication Provider (FCP) license from the CRA.⁸³

According to sources within Iran's ISP sector who spoke to ARTICLE 19 (who wished to remain anonymous), private companies have become interested in purchasing more capacity to provide more Internet traffic for users. For the first time in 20 years, Iranian authorities have allowed private companies to directly peer with international networks.

DECENTRALISATION CAUSES TENSION

This move towards decentralisation has caused tension between state agencies, and local media in Iran have been reporting ongoing disputes between the Ministry of ICT and entities aligned with the IRGC.⁸⁴

This dispute boils down to a fight over control over the network, in addition to profiting from a bigger share of revenues generated by communication companies. Although the dispute might sometimes be framed by the Ministry of ICT, and especially the concerted PR by Minister Azari Jahromi, as being pro-rights, Jahromi is affiliated with the Intelligence Ministry, which has long been known for abusing rights, including allegations against the Minister himself.⁸⁵ The dispute is more along the lines of who has access to profits, resources, such as data for social engineering,⁸⁶ or control over spectrum frequencies that could help develop 5G infrastructure.⁸⁷ Iran's telecommunication sector takes up an increasing portion of the nation's gross domestic product each year, with the market size more than doubling in the last 10 years.⁸⁸ Whomever controls this sector will have a massive role in shaping the future of Iran.

IRGC-owned Mobin Trust Consortium is TCI's majority shareholder, with a 36.99% stake in the company, followed by the government with 19.76%. TCI's own subsidiary MCI holds a 2.17% share in its parent company.⁸⁹

Although there was an edict by Supreme Leader Ayatollah Khamenei in January 2018 that the General Staff of the armed forces must give up the economic entities which they control that do not relate to their mission, this has been left up to broad interpretation.⁹⁰ It has not prevented companies loosely or indirectly affiliated with the IRGC from owning these entities.⁹¹

Furthermore, through lobbying MPs, the armed forces have tried to sideline the civilian government and increase their control over the network. The draft "Social Media Organisation" Bill, published in November 2018, proposed to cede control of the Internet gateways to the armed forces, removing it from the purview of the Ministry of ICT entirely. The Iranian Parliament's research centre later recommended that the control of Iran's Internet gateways be transferred to the SNSC instead of the armed forces. Either scenario would curtail the role of Iran's elected officials and the civilian government in devising Internet policy. This would mean less accountability in terms of decisions taken to implement Internet

shutdowns or other censorship decisions, leaving more room to abuse the vague notions of “national security” to repress rights, especially freedom of expression in the case of the Internet, during protests.

ISPs ENACT GOVERNMENT CENSORSHIP

ISPs have their own connectivity with the outside world, but still form an active part of the systems of censorship and surveillance dictated by authorities.

Iran's larger ISPs in the past few years are forced to buy Lawful Intercept (LI) equipment from the government and install it in their systems in order to be licensed by the CRA to operate.⁹² Relying on a “decentralised” system to implement the LI system to follow centralised control policies and decisions is a well-known tactic in countries with heavy surveillance and control tactics.

In Russia, authorities use SORM (System for Operative Investigative Activities) to monitor traffic, implement blocking of content, and monitor the data that flows across their network.⁹³ Iran has developed their monitoring systems in the same way. This system of data interception also sometimes creates inconsistencies in how censorship policies are applied, as some of these remote nodes in these ISPs do not get synced or updated at the same time.

For the smaller ISPs that do not have the resources and capacity to buy their own LI systems, network connectivity is achieved in conjunction with TIC technology. Transmissions rely on the TIC to implement the systems of censorship and surveillance while they receive the traffic through the international peerings (connections).⁹⁴

This, in effect, ensures that although they have a direct peering with a foreign ISP, the government can impose their censorship and surveillance through a system tied to the TIC as the network data is transmitted between the foreign connection and the smaller ISPs.

Chapter 4: Iran's Internet decisions



Although infrastructural changes have occurred since November 2019, the overall governance mechanisms that exist leave little hope for accountability and freedoms online. Ambiguity about the processes of Internet decisions are a hallmark of the overall governance system in Iran, as represented by our illustration of the decision-making flows in Figure 8. Different censorship events seem to elicit different routes, and there are no known protocols over what institutions are responsible for what decisions.

For example, in 2009 when Twitter and Facebook were censored in the weeks leading up to the presidential elections, the Committee Charged with Determining Offensive Content (CCDOC) (before it was ratified into the 2009 CCL) was responsible for making that decision. The momentary shutdowns of the 2009 protests stemmed from the SNSC.

ORDERING A SHUTDOWN

Under normal circumstances, and according to the CCL, filtering decisions have a legal framework.⁹⁵ They should follow decisions made in the multi-agency body of the CCDOC, which is situated within the judicial rather than security branch.

Shutdown decisions, meanwhile, have no clear legal framework, but only have precedent as occurring as national security decisions, which is why they are always made in the SNSC. According to the current precedent, the SNSC orders shutdowns, which are then implemented through to the Ministry of ICT. However, there is much ambiguity over where decisions originate in this multi-agency body.

It has been confirmed that Internet shutdowns and filtering of Telegram and Instagram⁹⁶ were ordered by the SNSC during the protests of December 2017 and January 2018. There was, however, added complexity to the decision process made in November 2019 when a subdivision of the SNSC – the NSC – was involved.

POWER STRUCTURES INVOLVED IN IRAN'S INTERNET DECISIONS

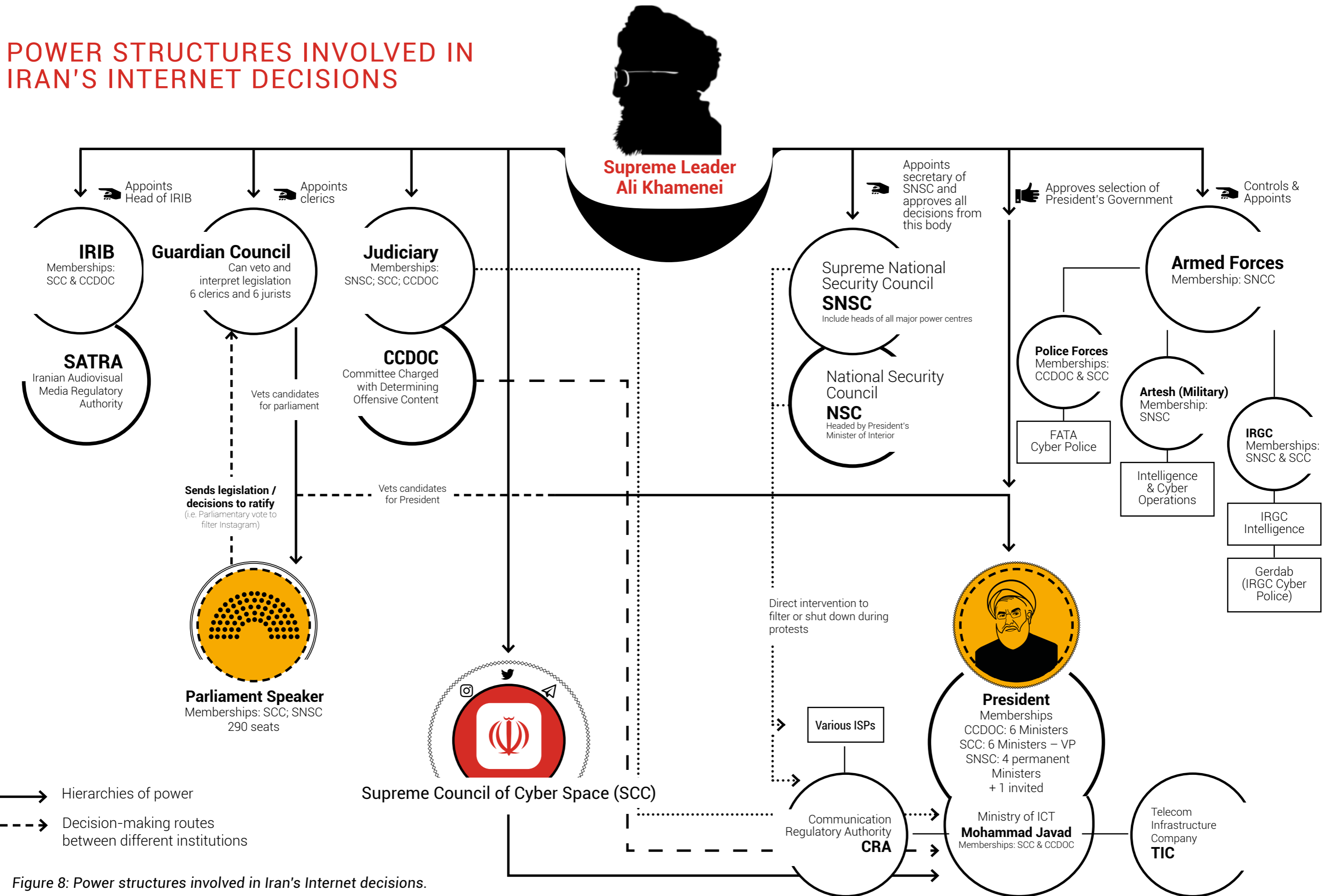


Figure 8: Power structures involved in Iran's Internet decisions.

INTERNET POLICY: WHERE DOES THE POWER LIE?

Ambiguities in the CRA

The CRA has a direct role applying the various forms of technical censorship in Iran. Licensing and regulation are part of its typical mandate. There are, however, unwritten (but well-known) rules within Iran's Internet network community; the reality is that their mandate goes beyond that.

The CRA has a division called the Office of Security of Communications Systems (OSCS) or اداره کل امنیت سیستم های ارتباطی that network operators in the country (such as data centres, ISPs, and other large networks in the country) know by the name of network security or امنیت شبکه.

The staff who run this division directly overlap with current or previous staff of the Ministry of Intelligence.⁹⁷ During his tenure working at the Ministry of Intelligence, Azari Jahromi was the head of this division (concurrent with his position as head of the TIC) before he became Minister of ICT.

Jahromi's current deputy minister and current head of TIC, Hamid Fatahi, now holds the post overseeing the OSCS within the CRA.⁹⁸ Jahromi and his team within the Ministry of ICT are known to have strong ties and allegiance to the Ministry of Intelligence.

This implicates the Minister and the entire Ministry of ICT in implementing the shutdown.

The NSC and Internet policy

The NSC has been a subordinate subcommittee of the SNSC since 1989 and is led by the Minister of Interior.⁹⁹

The NSC had remained mostly uninvolved in Internet policy until November 2019, but it was named as being responsible for the fuel hikes that led to the protests and the subsequent decision to shut down the Internet.¹⁰⁰

Although the SNSC is chaired by the President, and is a multi-agency body with many members from the semi-elected government on the council, decisions taken by the SNSC are thought to originate from those close to the Supreme Leader.

Members of the Rouhani Administration have been able to largely distance themselves from decisions made within the SNSC. For example, during previous protests, statements and announcements implied the responsibility behind the Internet disconnections and censorship did not come from their government.

Statements by the Minister of ICT, however, indicated he was trying to restore connections to the temporary blocks on Telegram and Instagram in January 2018 through the NSC, where he has some leverage, despite the decisions being made originally in the SNSC.¹⁰¹

Less transparency than ever?

There are major ambiguities related to the November 2019 shutdowns that make it hard to see who is ultimately responsible for this decision. Rouhani's Minister of Interior ultimately made the decision over when and if the fuel hikes would occur through his chairmanship of the NSC. Two questions remain unanswered: who influenced the decision to shut down the Internet? And was the Rouhani Administration directly culpable?

Protests and much of the narrative demonstrating anger for the fuel hikes were directed at Rouhani's Administration throughout the protests. However, Rouhani has (unsuccessfully) attempted to distance himself from the fuel decision, while acknowledging his Minister's central role.¹⁰²

An anonymous Iranian journalist covering politics told us:

“November 2019 was the first time we heard of the name of the NSC as a real political player. The BBC article was helpful in illustrating the difference between the NSC and the SNSC for the first time. It's believed the NSC was used during the 2019 protests specifically to use the Rouhani Administration as a scapegoat. It was used so the Supreme Leader and the larger SNSC could be distanced from the crackdown. Also, it indicated that the larger SNSC didn't get involved in decisions related to the protests to signal it was not a significant event within the broader politics and history of the Islamic Republic.”¹⁰³

The price hikes originated from the SNSC or elements close to it, if not the office of the Supreme Leader himself. However, the Supreme Leader has purposefully distanced himself from the hikes, indicating he “does not interfere” in the decision-making processes.¹⁰⁴ However, the administration, including the Minister of ICT, have tried to express their opposition, or at the very least distaste for the decision to shut down the Internet.¹⁰⁵

Within the SNSC, the decision to shut down the Internet would hypothetically have been taken with the counsel of the Minister of ICT, because as per Article 176 of the Constitution of the Islamic Republic of Iran, the Minister could have been called upon to offer his opinion on the decision.¹⁰⁶

The fact that there is no transparency and accountability in this decision-making process is a major issue within the laws and processes of Iran. Although the Minister of ICT was extremely vocal about his opposition to the shutdowns, he did not provide any clarity on his involvement at the NSC.

During the 2017/18 protests, the SNSC was involved in the temporary censorship of Telegram and Instagram, and also in providing instructions to the CRA to disconnect global connections at various moments during the protests.¹⁰⁷

However, this also received conflicting reports by authorities about how it was implemented. Some say the SNSC or the NSC gave the directions to the Ministry of

ICT's CRA, while other reports say those bodies directly contacted the ISPs to order the shutdowns. The decision to censor Telegram permanently in April 2018 came directly from Iran's judicial system, as opposed to the multi-agency CCDOC.¹⁰⁸

As of June 2020, momentum has started to build within the newly elected majority hard-liner parliament to censor Instagram.¹⁰⁹ If this decision does take place, it will be unprecedented in the history of Internet policy for such a decision to originate from parliament, and charts a new route for Internet decision-making in Iran (see the broken lines in Figure 8).¹¹⁰

CHANGING THE RULES FOR ORDERING AN INTERNET SHUTDOWN?

The Minister of ICT and his deputies have proposed to reform the system so that Internet shutdowns could only be implemented after a parliamentary vote, as opposed to an arbitrary decision of the SNSC.¹¹¹

The Ministry officials declared they were writing a bill for these changes, but there has been no update since December 2019. The proposed bill (which has yet to have a name or a draft) has given rise to severe concerns for freedom of expression and normalisation of states that will allow them to "shut down" the Internet through a vote.

RECOMMENDATIONS

ISLAMIC REPUBLIC OF IRAN

All state institutions responsible for decision-making and governance must recognise that the disconnection from the international Internet was an Internet shutdown incompatible with human rights law, and must ensure they do not reoccur.

The Islamic Republic of Iran must complete a transparent and independent investigation into the shutdown and hold accountable those who were responsible for violating human rights.

Iranian Ministry of ICT

The events of November 2019 are a serious violation of international human rights standards: those involved must be investigated and prosecuted and perpetrators and instigators brought to justice.

The Minister of ICT, and all other relevant officials, must be transparently and independently investigated for their participation in the decision-making bodies that enacted the censorship and shutdowns.

The Ministry of ICT must ensure that Iran does not enact any form of Internet shutdowns and cannot justify such actions through the ITU Constitution or parliamentary votes.

The Ministry must recognise such actions as violations of human rights, and especially freedom of expression within ICCPR, of which Iran is a signatory.

The Ministry must continue its efforts to decentralise Iran's Internet infrastructure, and facilitate the creation of a CRA that oversees Iran's Internet governance according to international human rights standards.

Supreme National Security Council

The SNSC must stop using national security as an excuse to infringe on the right to protest and the right to freedom of expression. The SNSC must stop ordering Internet shutdowns. The SNSC must transparently document the decisions to illustrate who is behind the opaque decision-making policies of the council, and highlight the differences that exist between who makes decisions in the SNSC and the NSC. The SNSC must publish information about composition and voting procedure within all its branches (SNSC or NSC).

Parliament

The parliament must pass laws that recognise access to the Internet as a human right. They must cease their ongoing discussions to block Internet applications such as Instagram.

Judiciary

The judiciary must only restrict freedom of expression online in accordance with international freedom of expression standards. Restrictions should have a sufficiently clear basis in law, and be necessary and proportionate to a legitimate aim under the ICCPR. The judiciary must reverse their order to block Telegram from April 2018.

Committee Charged with Determining Offensive Content

The CCDOC must reverse its order to censor Twitter and Facebook from 2009. It must refrain from making decisions to limit freedom of expression and access to information online, and must reform its mandate to tackle and remove offensive content that follows international standards for freedom of expression (i.e. content related to child pornography and cybercrime related to narcotics, fraud, or theft).

EUROPEAN UNION

The European External Action Service should engage in a dialogue with Iranian representatives. In particular, it should encourage Iran to reform its data protection regulations in line with international standards on privacy, including encouraging Iran to receive an adequacy decision through the GDPR.

The EU Commission's Units (i.e. Head of the International Data Flows and Protection Unit) responsible for enforcing GDPR should seek bilateral talks with the Islamic Republic of Iran to leverage the possibilities of data trade relationships through privacy and data protection reform.

UNITED STATES

The US should broaden the scope of General License D-1 within the Office of Foreign Assets Control (OFAC) in the Treasury Department to facilitate the export and provision of a wider range of services by US technology companies to Iran, such as through the Apple App store, or the Google Cloud Platform.

The US needs to examine the effects of its Maximum Pressure policy. One of the most obvious results of economic isolation is incentivising Iranian authorities towards a closed Internet system, and diminishing the costs of shutdowns from the global Internet. The US must reverse these isolationist policies, which provide more reasons for Iran to continue its plans for implementing the NIN.

As the US Department of State develops its policies on Iran, and continues to espouse the values of Internet policy, it must recognise that although Iran remains connected economically to the rest of the world, it also has an incentive to remain digitally connected to the rest of the world.

US policies of maximum pressure preclude the possibility for Iran to develop mechanisms to be engaged in international trade, or keep its citizenry and private sector connected to the global Internet.

TECHNOLOGY COMPANIES

US technology companies must recognise the centrality of their role in providing services within Iran. They must seek General License D-1 wherever possible, and offer both commercial and personal hosting in order to deliver secure hosting and platforms options within Iran (and prevent buy-in into the NIN). US technology companies must revisit all platforms they block inside Iran and work with OFAC to ensure whitelisting of their services to Iran.

INTERNATIONAL TELECOMMUNICATIONS UNION

The ITU must ensure its members stay vigilant towards international human rights law. They must condemn Internet shutdowns in all their forms.

ANNEX 1: IRAN'S INTERNET INFRASTRUCTURE 2019 AND 2020

IRANIAN INTERNET INFRASTRUCTURE MAP 2019

Domestic Peers / ISPs

The majority of the connections we see on this map are the "domestic peers" or domestic Internet Service Providers (ISPs) that are connecting homes, mobile networks, and institutions to domestic and international networks.

This is the first layer of Internet Service Providers (ISPs) that are connected directly to the international gateways. A second layer smaller ISPs connect through these "first layer" which are major providers, illustrated in this map.

TIC International Gateways

The Telecommunication Infrastructure Company (TIC) is the sole provider of IP communication infrastructure to all private and public operators in the Iran. TIC is also the sole party for all international gateways and IP capacity and connectivity services in the country. It sits under the Ministry of Information, Communication and Technology (ICT), which oversees all IP communication infrastructure across the country.

IPM International Gateways

Although not as large as the TIC Gateway, this older international gateway from the Institute for research in fundamental sciences (IPM), is the only other international gateway in Iran and serves the Internet to research and educational institutes.

International Transit Providers

International transit providers are companies providing international connectivity to the Iranian network, via the two gateways mentioned above.

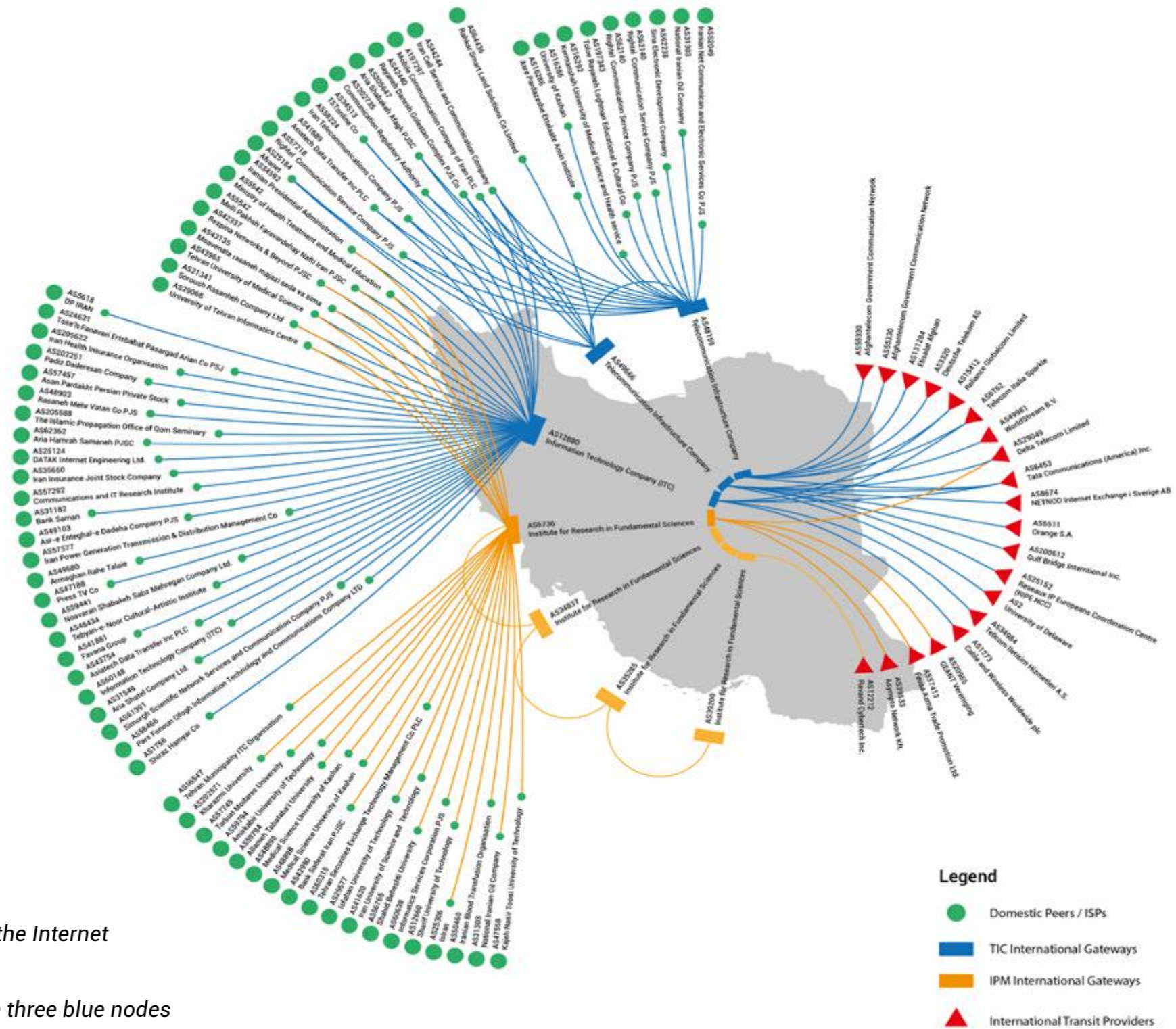


Figure A1.1: A map of Iran's Internet infrastructure at the time of the Internet shutdowns – November 2019*.

*The five gateways that peer to international connections are the three blue nodes and two orange nodes at the center of the graph.

AS34837 and AS35285 of IPM (also in orange) do not peer to international connections despite being part of the network.

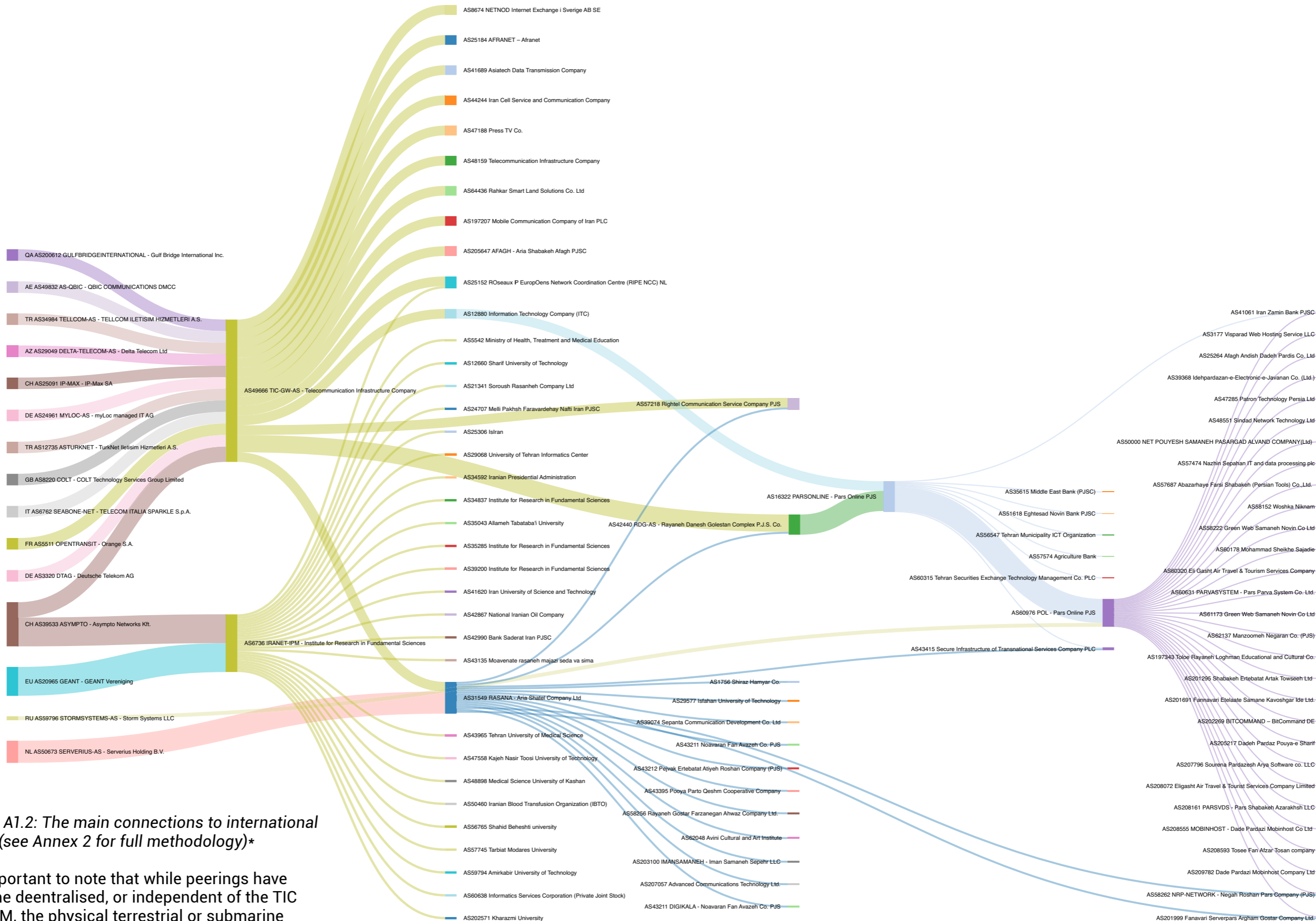


Figure A1.2: The main connections to international peers (see Annex 2 for full methodology)*

It's important to note that while peerings have become deentralised, or independent of the TIC and IPM, the physical terrestrial or submarine cables enabling these peerings are still operated by the TIC (or state authorities).

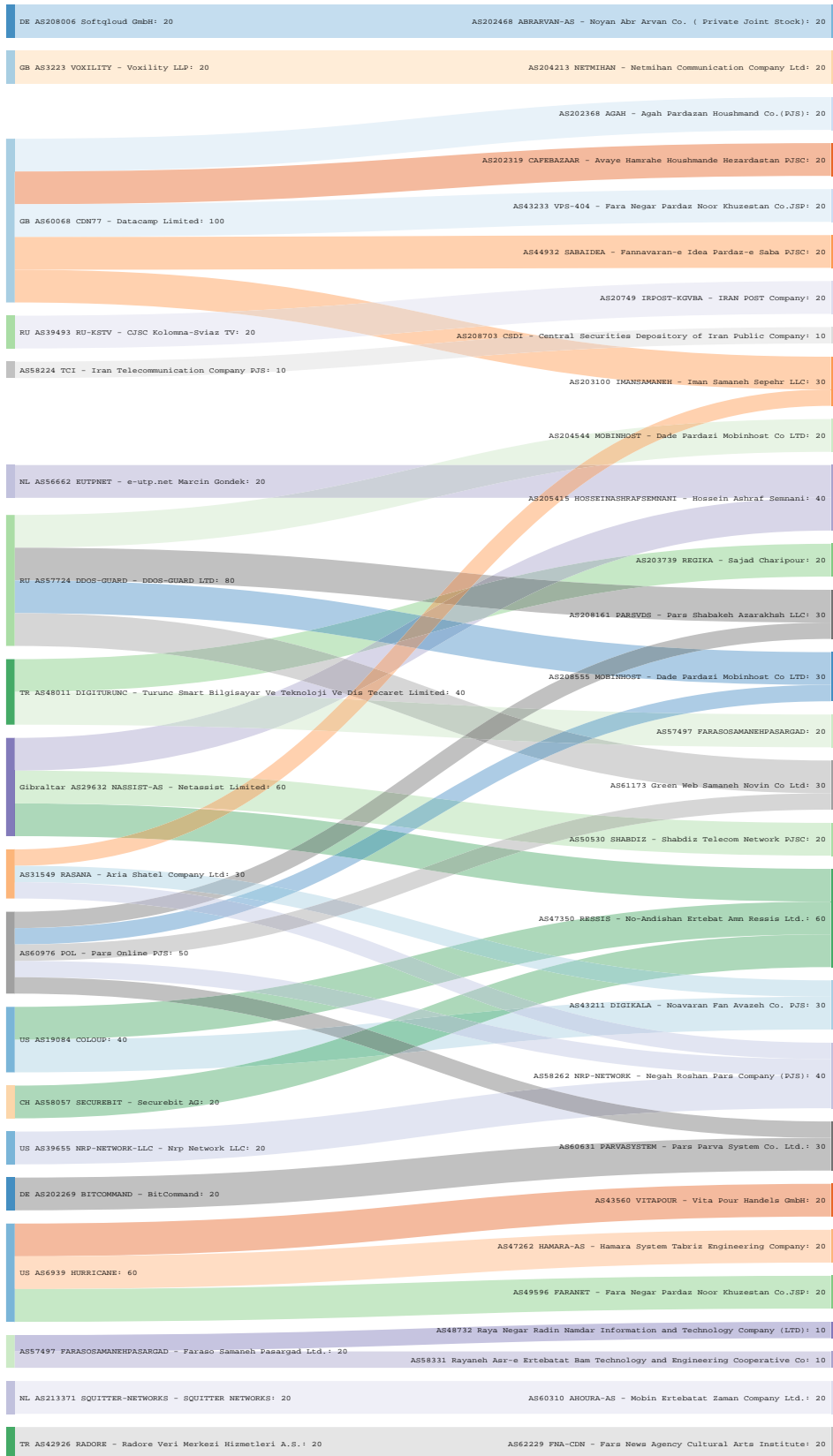


Figure A1.3: Smaller “first layer” connections. These are ISPs that are directly connecting to international gateways.

ANNEX 2: METHODOLOGY FOR ANNEX 1

In both these diagrams, we used public Border Gateway Protocol (BGP) data. An analogy to describe BGP is the “postal service of the Internet”.¹¹² A postal service is the fastest and most efficient route of delivering mail to its destination.

When someone submits data across the Internet, BGP finds the available paths the data can travel through and picks the best route, which means hopping between Autonomous Systems (AS). If BGP is the postal service, AS are individual post office branches (although not always part of the same organisation, unlike post offices).

AS belong to ISPs or other large high-tech organisations (including companies, universities, governments, and scientific institutions). Data is forwarded to an AS from internal routers. The AS then uses BGP routing to transfer the data to its destination.

Using BGP data, which is publicly available online, we mapped the international connectivity of the Iranian Internet infrastructure. The entire Iranian network is too large to show here, and so we limited the visualisation to the organisations (AS) that had significance in the network. The ISPs or organisations visualised have one or more of the following characteristics:

- Had an international peering / connectivity;
- Were a major ISP / data centre / node; and
- Had another significant presence in the network, i.e. international peerings with i.root and k.root servers.

ENDNOTES

INTRODUCTION:

- 1 "Iran: Details released of 304 deaths during protests six months after security forces' killing spree," Amnesty International, 20 May 2020, <https://www.amnesty.org/en/latest/news/2020/05/iran-details-released-of-304-deaths-during-protests-six-months-after-security-forces-killing-spreed/>; "Gunning them down: State violence against protesters in Iran," Centre for Human Rights in Iran, 26 May 2020, <https://iranhumanrights.org/wp-content/uploads/Iran-Human-Rights-November-2019-January-2020-Protests.pdf>
- 2 "Protests break out in two Iranian cities, Internet disrupted," Radio Farda, 16 July 2020, <https://en.radiofarda.com/a/breaking-news-protests-break-out-in-iran/30732043.html>
- 3 "Iran Internet 'disrupted' ahead of protests," BBC News, 25 December 2019, <https://www.bbc.co.uk/news/world-middle-east-50911457>
- 4 "Iran: Internet disruptions after online protests against death sentences for three young men," ARTICLE 19, 15 July 2020, <https://www.ARTICLE19.org/resources/iran-Internet-disruptions-after-online-protests-against-death-sentences-for-three-young-men/>
- 5 According to the latest ITU statistics from 2018, 70% of Iran's population are using the Internet, <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>
- 6 Alimardani, M. "Iran vows to block all unlicensed websites," Global Voices, 15 August 2014, <https://globalvoices.org/2014/08/16/iran-vows-to-block-all-unlicensed-websites/>
- 7 These were demonstrations against what were believed to be the fraudulent re-election of President Mahmoud Ahmadinejad.
- 8 "After the Green Movement: Internet controls in Iran, 2009-2012," Open Net Initiative, 15 February 2013, <https://opennet.net/blog/2013/02/after-green-movement-Internet-controls-iran-2009-2012>
- 9 Ibid.
- 10 "Tightening the net: Iran's national Internet project," ARTICLE 19, 29 March 2017, <https://www.article19.org/resources/tightening-the-net-irans-national-internet-project/>
- 11 Esfandiari, G. "Iran admits throttling Internet to 'preserve calm' during elections," RadioFreeEurope/RadioLiberty, 26 June 2013, <https://www.rferl.org/a/iran-Internet-disruptions-election/25028696.html>
- 12 Anderson, C. "Dimming the Internet: detecting throttling as a mechanism of censorship in Iran," 18 June 2013. <https://arxiv.org/abs/1306.436>
- 13 "Tightening the net: Internet controls during and after Iran's protests," ARTICLE 19, 8 March

2018, <https://www.ARTICLE 19.org/resources/tightening-net-Internet-controls-irans-protests/>

14 UN Human Rights Council Resolution A/HRC/res/32/13, June 2016, <http://bit.ly/2F2R8GE>

15 UN Human Rights Committee, General Comment No. 34. Article 19: Freedoms of opinion and expression, 2011, ACCPR/C/GC/34, para. 43, <https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>

16 "Independent rights experts sound alarm at Iran protest crackdown, Internet blackout," UN News, 22 November 2019, <https://news.un.org/en/story/2019/11/1051981>; "Iran protests: Live ammunition reportedly used, says UN human rights office," UN News, 19 November 2019, <https://news.un.org/en/story/2019/11/1051661>

17 Iran ICT Minister argues that ITU constitution sanctions Internet shutdowns," ISNA, 14 December 2019, <https://www.isna.ir/news/98092317231>

18 Article 34: Stoppage of Telecommunications, 180, PP-98:

1. Member States reserve the right to stop, in accordance with their national law, the transmission of any private telegram which may appear dangerous to the security of the State or contrary to its laws, to public order or to decency, provided that they immediately notify the office of origin of the stoppage of any such telegram or any part thereof, except when such notification may appear dangerous to the security of the State.

2. 181, PP-98: Member States also reserve the right to cut off, in accordance with their national law, any other private telecommunications which may

appear dangerous to the security of the State or contrary to its laws, to public order or to decency.

Article 35: Suspension of Services, 182, PP-98:

Each Member State reserves the right to suspend the international telecommunication service, either generally or only for certain relations and/or for certain kinds of correspondence, outgoing, incoming or in transit, provided that it immediately notifies such action to each of the other Member States through the Secretary-General.

19 §1.3: Values, 5, ITU Strategic Plan for the Union 2020–2023. https://www.itu.int/en/council/planning/Documents/ITU_Strategic_plan_2020-2023.pdf

20 C.f. Article 34 para 1 and Article 39 para 1 of the ITU Constitution. <https://www.itu.int/en/council/Documents/basic-texts/Constitution-E.pdf>

CHAPTER 1:

21 See page 4 in "Time frame of killings in Iran: Details of 304 deaths in crackdown on November 2019 protests," Amnesty International, 20 May 2020, <https://www.amnesty.org/download/Documents/MDE1323082020ENGLISH.PDF>

22 "Iran blocks nearly all Internet access," *The New York Times*, 17 November 2019. <https://www.nytimes.com/2019/11/17/world/middleeast/iran-protest-rouhani.html>

23 "Islamic Republic of Iran's Human Rights Commission: the Internet was not shut down," *Tasnim News*, 4 December 2019. <https://www.tabnak.ir/003wyYak.ir/003wyY>

- 24 "Time 100 Photos: The Death of Neda," *Time Magazine*, <http://100photos.time.com/photos/death-of-neda>
- 25 "Iran state TV says 'rioters' shot and killed in last month's protests," *The Guardian*, 3 December 2019, <https://www.theguardian.com/world/2019/dec/03/iran-state-tv-says-rioters-shot-and-killed-in-last-months-protests>. For documentation of satellite jamming, see "Rises in the price of petrol are fuelling unrest in Iran," *The Economist*, 21 November 2019, <https://www.economist.com/middle-east-and-africa/2019/11/21/rises-in-the-price-of-petrol-are-fuelling-unrest-in-iran>
- 26 Ibid.
- 27 See page 4 "Time Frame of Killings". "Iran: Details of 304 Deaths in Crackdown on November 2019 Protests," Amnesty International, 20 May 2020, <https://www.amnesty.org/download/Documents/MDE1323082020ENGLISH.PDF>
- 28 Internet Intelligence is powered by Oracle Cloud Infrastructure. They analyse the connectivity of every network and every service provider in the world.
- 29 Ibid.
- 30 "The Internet in Khuzestan and Sistan and Balochistan remains offline," ISNA, 3 December 2019, <https://www.isna.ir/news/98091208063/>

CHAPTER 2:

- 31 "Myanmar: One year on, Internet shutdown imperils human rights in Myanmar," ARTICLE 19, 19 June 2020, <https://www.ARTICLE19.org/resources/myanmar-one-year-on-Internet-shutdown-imperils-human-rights-in-myanmar/>; "HRC44: Cease Internet shutdowns during protest," ARTICLE 19, 10 July 2019, <https://www.article19.org/resources/hrc44-cease-Internet-shutdowns-during-protest/>; "Targeted, cut off, and left in the dark" Access Now, 2020, <https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf>.
- 32 "Tightening the Net: Iran's National Internet Project," ARTICLE 19, 29 March 2017.
- 33 Kalbasi, K. "Iranians endure Internet shutdown with despair and disarray," 25 November 2019, <https://www.atlanticcouncil.org/blogs/iransource/iranians-endure-Internet-shutdown-with-despair-and-disarray/>
- 34 A former head of Iran's Chamber of Commerce, Mohessen Jalalpour, estimates that the blackout cost the Iranian economy USD1.5 billion. He told Khabaronline: "The Internet shutdown cut us off from communicating with our foreign partners. We simply were not able to answer emails. Using telephone services and fax for business communications has become a thing of the past." <https://www.khabaronline.ir/news/1323822> Netblocks reported that the Internet shutdown cost Iran USD369.5 million a day or USD15.4 million per hour. <https://netblocks.org/cost/>

- 35 Alimardani, M. "Stuxnet, American sanctions, and cyberwar are legitimizing Iranian Internet controls," *Vice*, 3 July 2019, https://www.vice.com/en_us/article/vb9859/stuxnet-american-sanctions-and-cyberwar-are-legitimizing-iranian-Internet-controls
- 36 "US repeal of net neutrality harms Internet freedom at home and abroad," ARTICLE 19, 21 December 2017, <https://www.ARTICLE19.org/resources/us-repeal-net-neutrality-harms-Internet-freedom-home-abroad/>
- 37 Kalbasi, K. "Fiery debate on fate of local messengers, Iran's national intranet," *Financial Tribune*, 17 December 2019, <https://financialtribune.com/articles/sci-tech/101263/fiery-debate-on-fate-of-local-messengers-iran-s-national-intranet>
- 38 A 2019 poll by the Iranian Students Polling Agency (ISPA) has the most used applications in Iran as WhatsApp, Telegram, and Instagram, <http://ispa.ir/Default/Details/fa/2095>.
- 39 Jafari, H. "Iranian search engines to know about," *Techrasa*, 10 March 2016, <http://techrasa.com/2016/03/10/4-iranian-search-engines-to-know-about/>
- 40 Although national search engines existed, they relied on Google's application programming interface (API). As one developer in Iran told ISNA News: "These events showed we do not have a national search engine and the existing ones used the Google API, and as the Internet went down and Google became unavailable, they showed strange results, either results such as Wikipedia pages that were not available or results that were completely irrelevant." See "Reasons for the inefficiency of search engines when the Internet went down," ISNA News, 5 December 2019. <https://www.isna.ir/news/98091409969>
- 41 This January 2019 article on Iran's Digiato Technology News website analyses the success of local technology platforms such as Aparat to only be a result of Iran's censorship of YouTube. See Mostakin, A. "Why is the presence of Aparat as part of the top 100 most visited sites in the world not happy news for Iranians?" Digiato, 19 January 2019, <https://dgto.ir/16wo>; "Which sites are included in the list of discounted websites?" ISNA, 18 May 2020, <https://www.isna.ir/news/99022920494/>; A government list of subsidised websites: https://g2b.ito.gov.ir/index.php/site/list_ip
- 42 "Iran: National messenger apps are the new hallmark of Internet nationalisation," ARTICLE 19, 21 October 2018, <https://www.ARTICLE19.org/resources/iran-national-messenger-apps-are-the-new-hallmark-of-Internet-nationalisation/>; Jafari, H. "Million dollar incentives for local messaging apps in Iran," *Techrasa*, 25 February 2017. <http://techrasa.com/2017/02/25/million-dollar-incentives-local-messaging-apps-iran/>
- 43 "Barring use of foreign messengers within institutions of the government," ISNA, 28 February 2020, <https://www.isna.ir/news/97012911021/>;
- 44 Anonymous Iran-based sources have confirmed this with ARTICLE 19.
- 45 Tehran resident and technology entrepreneur Arash Zad tweets on 23 November 2019: "One of the most disgusting opportunistic actions of last week, these highway billboards of Balad that quickly mushroomed

- two to three days after the start of the Internet shutdowns. Profiting off the censorship placed on people. This is happening today and has always happened." <https://twitter.com/arashzd/status/1198300724741971969?s=20>
- 46 "The launch of a working group to combat American sanctions at the National Centre for Cyberspace," IRNA News, 13 May 2019, www.irna.ir/news/83312564/; see also Alimardani, "Stuxnet, American sanctions, and cyberwar are legitimizing Iranian Internet controls," Vice, 3 July 2019, https://www.vice.com/en_us/article/vb9859/stuxnet-american-sanctions-and-cyberwar-are-legitimizing-iranian-Internet-controls
- 47 Alimardani, "Stuxnet, American sanctions, and cyberwar are legitimizing Iranian Internet controls," Vice, 3 July 2019.
- 48 "The launch of a working group" IRNA News.
- 49 Ibid.
- 50 This was a legacy of the 2009 Internet shutdown where petrol stations, banks and businesses essential for day-to-day activity were disrupted during the shutdown. All these companies, non-governmental organisations, and large government entities were required to join the NIN.
- 51 "Tightening the Net: Iran's National Internet Project."
- 52 "American Servers Sanctioned Hosting .ir Domains", 598 News Agency, 23 June 2011, <http://www.598.ir/fa/رآی-آت-اد-هن-م-اد-م-ی-رحت-14647/news>
- 53 "The launch of a working group" IRNA News.
- 54 "More Iranians forced to rely on unsafe online hosting after Amazon ban," Centre for Human Rights in Iran, 7 August 2019, <https://iranhumanrights.org/2019/08/more-iranians-forced-to-rely-on-unsafe-online-hosting-after-amazon/>
- 55 "Passive Defence Organisation discusses possibility of US embargo on Internet," Tasnim News, 21 October 2018, <https://www.tasnimnews.com/fa/news/1397/07/29/1857808>
- 56 "The possibility for America to block the Internet for us does not exist," Peivast, 23 October 2018, <https://peivast.com/p/62668>
- 57 "What do Internet sanctions mean?" Hamshahri Online Newspaper, 28 October 2018, <http://sharghdaily.com/fa/main/detail/198593>
- 58 "Apple appears to have totally cut off Iran from the App Store", The Verge, 15 March 2018, <https://www.theverge.com/2018/3/15/17126342/apple-iran-app-store-block>
- 59 "Apple unblocks App Store for Iranians again", *Financial Tribune*, 16 March 2018; <https://financialtribune.com/articles/economy-sci-tech/83656/apple-unblocks-app-store-for-iranians-again>
- 60 "Silicon Valley preaches diversity and inclusion while excluding Iranians", Alimardani, Mahsa & Pakzad, Roya, Atlantic Council, 8 April 2019.
- 61 "More Iranians forced to rely on unsafe online hosting after amazon ban," Centre for Human Rights in Iran, 7 August 2019, <https://iranhumanrights.org/2019/08/more-iranians-forced-to-rely-on-unsafe-online-hosting-after-amazon/>

- 62 See note 28.
- 63 Tajdin, B. "Iran letter raises prospect of white list Internet clampdown," BBC News, 26 November 2019, <https://www.bbc.co.uk/news/technology-50563917>
- 64 "Russia has banned LinkedIn," CNN, 17 November 2016, <https://money.cnn.com/2016/11/17/technology/russia-linkedin-banned/index.html>; "Russian court fines Twitter and Facebook 62,840 dollars each for refusing to localize user data," Meduza, 13 February 2020. <https://meduza.io/en/news/2020/02/13/russian-court-fines-twitter-62-840-dollars-for-refusing-to-localize-user-data>
- 65 At the time of writing, the debates to ban the TikTok application in the US are ongoing. President Trump has encouraged Microsoft's purchase of the company for its Chinese owners in order to remain uncensored in the US. Human rights concerns arise from the fact that censorship or forced localisation of the application is neither necessary nor proportionate to legitimate security concerns over the application. It is unclear how much of the issue is American protectionism, legitimate fear of surveillance, foreign influence, or just Chinese xenophobia.
- 66 Tightening the Net: A New Cabinet and New Attempts at Control, Appendix 1
- 67 MJ Azari Jahromi, ICT Minister of Iran tweeted on 25 May 2018: "Congratulations to @EU_Commission on the implementation of #GDPR, A comprehensive Data Protection rule! I'm also looking forward to passing the #DataProtection Bill next month and conducting constructive talks with the EU about mutual legal & technical assistance", <https://twitter.com/azarijahromi/status/999968731852877824?s=2>
- 68 Articles of the GDPR: Processing of freedom of expression and information; available at: <https://bit.ly/2MLN3Gz>
- 69 The Special Rapporteur on the situation of human rights in the Islamic Republic of Iran; the Special Rapporteur on the right to peaceful assembly and association; the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; and the Special Rapporteur on extrajudicial, summary or arbitrary executions. "Independent rights experts sound alarm at Iran protest crackdown, Internet blackout," UN News, 22 November 2019, <https://news.un.org/en/story/2019/11/1051981>; "Iran protests: Live ammunition reportedly users, says UN human rights office," UN News, 19 November 2019, <https://news.un.org/en/story/2019/11/1051661>
- 70 "Comments from the Human Rights Commission in response to the international commission of human rights about recent unrest," IRNA, 4 December 2019, www.irna.ir/news/83581211/
- 71 "Minister of ICT: we are looking to reconnect the Internet/we recognize the concerns of the people," ISNA, 18 November 2019, <https://www.isna.ir/news/98082717796/>
- 72 "Rouhani pledges stronger domestic intranet to cut need for the Internet", Radio Farda, 9 December 2019 <https://en.radiofarda.com/a/30314456.html>

- 73 See Tweet of Presidential Communications Deputy Alireza Moezzi: https://twitter.com/ar_moezi/status/1203601620258508800
- 74 "Preparing a bill where only the parliament can decide if the country implements a Internet shutdown," Tabnak, 28 November 2019, <https://tabnakjavan.com/fa/news/11576>
- CHAPTER 3:**
- 75 See the connections for universities that largely stayed online on the next page.
- 76 Many of these companies have deep ties to state-affiliated agencies, while some of them are owned by state-affiliated front companies.
- 77 "Jahromi's address to parliament: the Ministry's intentions for the National Information Network and ongoing space plans," Digiato, 21 June 2020, <https://dgto.ir/1qnc>
- 78 "Boosting Internet quality hinges on breaking up TCI's monopoly: Deputy ICT Minister Fatahi" Peivast, 1 July 2020, <https://peivast.com/p/80040>
- 79 "Telecommunication Company of Iran Relents, agrees to share infrastructure with ISPs," *Financial Tribune*, 4 February 2018, <https://financialtribune.com/articles/sci-tech/81382/telecommunication-company-of-iran-relents-agrees-to-share-infrastructure>
- 80 Minister of ICT Azari Jahromi via Twitter, <https://twitter.com/azarijahromi/status/934423809272270848?s=20>
- 81 "Tightening the Net: A new cabinet and new attempts at control."
- 82 "ISP mergers to challenge state-backed Telecom Co.," *Financial Tribune*, 31 October 2017, <https://financialtribune.com/articles/sci-tech/75316/isp-mergers-to-challenge-state-backed-telecom-co>
- 83 CRA link to the permit: <http://dastaviz.ir/fa/cra/>. This link doesn't work outside Iran but can also be found here: <https://asnad.cra.ir/Public/Documents/Details/0bccb54b-f687-e511-973c-68b599781b58>
- 84 Although the IRGC side of the dispute is covered by media such as Tasnim News, known to be affiliated to the IRGC, the Minister of ICT relies on his twitter and public statements to push his side.
- 85 "Tightening the Net: A new cabinet and new attempts at control."
- 86 The harvesting of data from Telegram forks allegedly belonging to the Ministry of Intelligence (closely aligned with Minister Azari Jahromi) became well known when the data leaked in 2020. <https://www.bloomberg.com/news/articles/2020-04-17/data-breach-shows-iranians-use-chat-apps-to-spy-researchers-say>
- 87 "Iran's state broadcaster withholding frequencies needed for Internet expansion," Radio Farda, 21 April 2020, <https://en.radiofarda.com/a/iran-s-state-broadcaster-withholding-frequencies-needed-for-Internet-expansion/30567822.html>
- 88 "Iran's telecommunications industry market size 2009–2020," Statista Research Department, 2020. <https://www.statista.com/statistics/557267/iran-telecom-industry-size/>
- 89 All stock data is publicly available on the Tehran Stock Exchange: tsetmc.com

- 90 "Khamenei orders IRGC to reduce controversial involvement in economy," Radio Farda, 21 January 2018, <https://en.radiofarda.com/a/iran-khamenei-irgc-economic-role/28987830.html>
- 91 "IRGC denies knowledge of Khamenei's edict on armed forces' role in economy", Majidyar, Ahmad, Middle East Institute, 25 January 2018, <https://www.mei.edu/publications/irgc-denies-knowledge-khameneis-edict-armed-forces-role-economy>
- 92 Although there is not a direct source to back this claim, evidence from various vendor agreements and cases like Nokia Siemens, alongside testimonies for the ISP industry prove the existence of Iran's use of LI equipment. See "Special Report: Chinese firm helps Iran spy on citizens," Reuters, 22 March 2012, <https://www.reuters.com/article/us-iran-telecoms/special-report-chinese-firm-helps-iran-spy-on-citizens-idUSBRE82L0B820120322>
- 93 Polyakova, A. "Russia is teaching the world to spy," *The New York Times*, 5 December 2019, <https://www.nytimes.com/2019/12/05/opinion/russia-hacking.html>
- 94 This information was received from anonymous testimonies from individuals working in Iran's ISP sector.

CHAPTER 4:

- 95 "Islamic Republic of Iran: Computer Crimes Law," ARTICLE 19, 2012, <https://www.article19.org/data/files/medialibrary/2921/12-01-30-FINAL-iran-WEB%5B4%5D.pdf>
- 96 They were unfiltered in January, but Telegram was permanently filtered in April 2018.
- 97 "In 2009, within the Ministry of Intelligence, I was the head of Office of Security of Communications Systems for the Communications Regulatory Authority," *Setare Sobh Newspaper*, 14 August 2017, <http://www.setaresobh.ir/fa/news/main/7924>
- 98 "Engineer Hamid Fatahi becomes the caretaker of Office of Security of Communications Systems (OSCS) within the Communication Regulatory Authority," Ministry of ICT, 3 September 2017, <https://www.ict.gov.ir/ir/news/25028>
- 99 On 28 July 1989, the IRI Constitution was reformed. A clause was added to the constitution and the SNSC was created by merging the NCS and Defense Council. Since then, the NSC has operated as an arm of SNSC. The text calls it a sub-council/subcommittee. See "Rahman Fazli: the head of the National Security Council," *Hamshahri*, 6 November 2013, hamshahronline.ir/x435x
- 100 President Rouhani is quoted by ISNA as saying on 2 December 2019: "I delegated the decision on how and when to implement the fuel price hike to the Interior Minister and the National Security Council," <https://www.isna.ir/news/98091007007>; Rouhani claims that the decision to implement a fuel price hike was ratified by the government, judiciary, and Majlis.
- 101 "Excerpts from the Minister of ICT's discussions on the filtering of Telegram," ISNA, 28 April 2018, <https://www.isna.ir/news/97020804738/>
- 102 "Rouhani says he did not know about the fuel price hikes that led to the November protests," RFERL, 27 November 2019, <https://en.radiofarda.com/a/rouhani-says-he-did-not-know-about-fuel-price-hike-that-led-to-protests/30295476.html>

- 103 "What is the National Security Council?" BBC Persian, 27 November 2019, <https://www.bbc.com/persian/iran-features-50472083>
- 104 "Statement of the Supreme Leader of the Revolution on the issues that arose after the implementation of the fuel consumption management plan," [Khamenei.ir](https://farsi.khamenei.ir/news-content?id=44020), 17 November 2019, <https://farsi.khamenei.ir/news-content?id=44020>
- 105 "Video: apology of the Minister of ICT for the Internet shutdown," ISNA, 24 November 2019, <https://www.isna.ir/news/98090301375/>
- 106 See members of the Council in Chapter 13 Article 176 of the Islamic Republic of Iran Constitution, <https://www.wipo.int/edocs/lexdocs/laws/en/ir/ir001en.pdf>
- 107 "Iran's severely disrupted Internet during protests 'websites hardly open'," Centre for Human Rights in Iran, 2 January 2018, <https://www.iranhumanrights.org/2018/01/irans-severely-disrupted-Internet-during-protests-websites-hardly-open/>
- 108 Iran later arrested the prosecutor who ordered the filtering of Telegram on corruption charges in October 2019, <https://apnews.com/fd6cbede80b94bbd8f7c950f6bfc2920>; Rouhani also complained the judiciary decision circumvented legal processes for censorship in Iran, <https://www.isna.ir/news/97021106718/>
- 109 "Iran's conservative parliament moves to ban Instagram," Al Monitor, 29 June 2020, <https://www.al-monitor.com/pulse/originals/2020/06/iran-conservative-parliament-ban-instagram.html>
- 110 Other analysis, including this Peivast report on a possible Instagram filtering, has suggested it would be a move urged by parliament but ultimately decided on by the Iranian judiciary, <https://peivast.com/p/81135>
- 111 "Preparing a bill where only the parliament can decide if the country implements an Internet shutdown," IRNA, 27 November 2019, <https://www.irna.ir/news/83571942>

ANNEX 2:

- 112 "What is BGP? BGP routing explained," Cloudflare, <https://www.cloudflare.com/learning/security/glossary/what-is-bgp/>



article19.org