



RESEARCH ARTICLE

Digital protectionism and national planning in the age of the internet: the case of Iran

Altug Yalcintas^{1*}  and Naseraddin Alizadeh² 

¹Department of Economics, Faculty of Political Sciences, Ankara University, 06590 Cebeci, Ankara, Turkey and ²Department of International Relations, Faculty of Economic and Administrative Sciences, Karabuk University, 78050 Kilavuzlar Koyu, Karabuk, Turkey

*Corresponding author. Email: altug.yalcintas@politics.ankara.edu.tr

(Received 24 October 2019; revised 11 February 2020; accepted 12 February 2020; first published online 19 March 2020)

Abstract

What do regulations in the developing world tell us about the internet economy? In this paper, we argue that the ways in which developing nation states adjust to and legislate the internet depends upon whether they possess a national planning strategy for international data traffic. Focusing our attention on the global trade of intangible goods in Iran, we aim to demonstrate that digital protectionism causes, to varying degrees, suppression, censorship, and the violation of freedom of speech and other civil rights on the internet. Our results show that digital protectionism generated an emergence of domestic start-ups, with companies, such as Facenema and Soroush, operating in the Iranian market in the absence of global rivals such as Facebook and WhatsApp. Yet, digital protectionism and sanction-induced barriers have triggered social problems, besides the emergence of parastatals, securing the economy to an inefficient social and economic path towards digital development.

Key words: Censorship; digitisation; import substitution; internet economy; Iran; sanction

What do regulations in the developing world tell us about the internet economy? In this paper, we argue that the ways in which developing nation states adjust to and legislate the internet depends upon whether they possess a national planning strategy for international data traffic. Focusing our attention on the global trade of intangible goods in Iran, we aim to demonstrate that digital protectionism causes, to varying degrees, suppression, censorship, and the violation of freedom of speech and other civil rights on the internet. The fact that development of cyberspace technology in Iran was contingent upon the necessities of the cyber and propaganda war with Western countries, as the pioneers of globalised economy, caused Iranian domestic cyberspace to be shaped in odd with the world order. The significant role played by the social media during violent uprising in 2009, 2017–2018, and 2019 gave upper hand to the hardliners who support the National Information Network (NIN) and domestic social media. Our results show that digital protectionism generated an emergence of domestic start-ups operating in the Iranian market in the absence of global rivals. Yet, digital protectionism and sanction-induced barriers have triggered social problems, besides the emergence of parastatals, securing the economy to an inefficient social and economic path towards digital development.

1. Digital protectionism in perspective

As a commodity, data travel the globe following routes resembling the roads built for the international trade of tangible goods. Web 2.0 platforms such as Google, Facebook, Twitter, Amazon, and Instagram build the highways and the gates, alongside the traffic protocols users are required to observe while

using the internet. Web 2.0 platforms do not provide the content; instead, they offer an infrastructure for users to produce, share, and consume contents under intellectual property protection. For nearly two decades, individuals around the globe have used Web 2.0 platforms so frequently that they have now transformed into digital monopolies, able to monitor every single movement by its users on the internet (Zuboff, 2019).

As Laura DeNardis (2014: 1) argues, ‘the diffuse nature of internet governance technologies is shifting historic control over these public interest areas from traditional nation-state bureaucracy to private ordering and new global institutions’. In the face of such developments, many of states turn into digital monopolies to empower their sovereignty (Bulut, 2016; Everard, 2000; Kohl, 2017; Lu and Liu, 2018; Sunstein, 2017). Today, developing nations such as China, Russia, Iran, and Turkey have adopted policy measures to track the internet economy and advance sophisticated tools, for example, through installing malicious software on the devices of individuals without their consent, organising cyber-attacks, and interfering in the democratic processes of other nations, such as general elections and referenda (Marczak *et al.*, 2018).¹

Subsequently, the importance of the internet economy for the nation state has necessitated the introduction of digital protectionism or policies aimed at localising data by preventing its transference internationally. According to Aaranson (2018), ‘digital protectionism is a broad term that refers to a wide range of barriers both to e-commerce and to cross-border data flows’ (see also Aaranson, 2016a, 2016b). Governments adopt protectionist policies in order to decrease the dependency of nations on digital media corporations collecting, storing, and commodifying user data.

What is it that makes data special? An internet economy creates added value when tangible goods are bought and sold on online retail shopping sites such as Amazon and Walmart, but then additionally, through digital media corporations commodifying the data produced by online users. These data include emails and messages posted on digital media websites, coupled with the metadata of each item traded on the internet, such as clicks, page views, and user profiles containing age, gender, and country of origin. Known as cookies, files are stored on the hard drives of individual users allowing corporations to monitor:

- (a) the location *where* websites were accessed,
- (b) *which* pages users visited,
- (c) *when* they visited these sites, and
- (d) *how much* time and money were spent on each webpage (Turow, 2011).

Since the advent of the Internet of Things, physical devices connected to each other have similarly enabled corporations to collect, store, and exchange data about the types of equipment an individual owns, how frequently they are used, and where they are located.

Nation states not only desire to control the global trade of hardware, computers, and mobile phones but likewise the global processes of data commodification, offering protectionist policies encouraging ‘local’ digital media corporations to store their user data within their specific national borders. Furthermore, nation states block digital media websites and impose taxes on their transactions allowing for ‘local’ corporations to advance their own technologies. In many high-income economies, nation states either employ geo-blocking techniques or block websites violating its laws of anti-trust and intellectual property.

Governors and ‘local’ media companies may see protectionist policies as the best measure to diminish a national economy’s dependence on foreign corporations. However, the lessons economists learnt

¹See ‘Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election’, Press Release. Available online at <https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election> and ‘Facebook/Cambridge Analytica: MEPs Pursue Personal Data Breaches Probe’, European Parliament Press Release. Available online at <http://www.europarl.europa.eu/news/en/press-room/20180530IPR04607/facebook-cambridge-analytica-meps-pursue-personal-data-breaches-probe>.

from the implementation of protectionist policies in the developing world suggest that protectionism may not always prove the best way for a nation to achieve growth rates in certain industries. One of the consequences of protectionism on the internet is that it engenders a large-scale emergent phenomenon termed *import substitution digitalisation*. As a reworked form of the policy of import substitution industrialisation that dominated the Global South from the 1950s until the 1980s (Ahmad, 1978; Baer, 1972; Cockcroft *et al.*, 1972), import substitution digitalisation is a strategy for regulating the internet whereby nation states implement protectionist policies. This often involves encouraging 'local' digital media corporations to store, analyse, and commodify their data within their national borders, despite such data being collaboratively produced by digital media users across various countries. It is frequently argued that the policies of import substitution promote labour productivity by creating incentives for 'infant industries' (Chang, 2002) to invest in research and development. In the case of digitalisation, however, import substitution does not always cause freedom of speech other civil rights on the internet although it can lead to a number of 'local' companies to operate in the internet economy in the absence of global rivals.

Nation states are not uniform, adopting various policies to safeguard the political interests of those in power. Nevertheless, many, if not all, nation states across the globe implement protectionist policies. Historically, nation states have regulated not only their sectors of oil and gas production, electricity, and financial services (Guerriero, 2019) but moreover, their television, radio, film, and recorded music industries (Lourenço and Turner, 2019; Mazzucato, 2011). If the politics of a nation have historically favoured government intervention, it is expected that a government may implement protectionist policies on the internet for regulating the international trade of digital commodities, such as with the 'Great Firewall of China', Russia's 'Sovereign Internet', Turkey's 'local and national Internet', and the 'National Information Network' in Iran. Consequently, when states are motivated for economic or security reasons, it is initially unrealistic to expect they may develop non-protectionist policies.

When nation states implement digital protectionism, one of the most common practices is the blocking or restricting of access, temporarily or partially, to the websites of large internet corporations mostly registered in the USA, such as Google, Facebook, Twitter, Instagram, WhatsApp, YouTube, Uber, and PayPal. China, Russia, Iran, and Turkey, among others, frequently claim that these corporations either evade their respective laws of taxation and confidentiality or break the rules of fair competition (Calder, 2017). As demonstrated in Table 1, the left column identifies which large digital corporations are blocked by several nation states to ensure that their citizens use 'local' alternatives. The right column displays some of the 'local' websites that nation states allow or encourage their citizens to use.

Iran imposes large scale controls on data and information mobility. Taking the country as a case study, we aim to examine the nature and consequences of digital protectionism and state-led planning. Specifically, we want to resolve the following question: What can regulations in Iran tell us about the internet economy in the developing world?

Despite the advantages of cross-country studies for understanding global trends in the internet economy, such studies often neglect the role and significance of country-specific factors shaped by the evolution of institutional conditions and economic outcomes at the national level. We argue these factors are rooted in global developments in the internet economy, together with each specific country's geopolitical challenges, economic structures, and historical contingencies. For instance, in Iran, access to considerable oil incomes and rents (Mohaddes and Pesaran, 2013) combined with the regime's factional nature (Alamdari, 2005) generated numerous opportunities for extensive state interventions in the economy. Factors such as rapid oil price changes, social unrest, and media wars have compelled the government to regulate the markets. Eventually developing into a player in the internet economy worth 40,000 billion Tomans as of 2017 (about 12 billion USD),² the

²<https://bit.ly/2sfybeL>.

Table 1. Digital protectionism in China, Russia, Iran, and Turkey

Digital media platforms	Digitally protected alternatives
Google.com (US)	Baidu.com (China); Yandex.ru (Russia); Yaani.com.tr (Turkey)
Gmail.com (US)	Mail.ru (Russia); Mail.qq.com (China); Yaanimail.com (Turkey)
Facebook.com (US)	Vk.ru (Russia); Renren.com (China), Cloob.com (Iran)
Twitter.com (US)	Weibo.com (China)
Youtube.com (US)	Youku.com (China); Aparat.com (Iran)
Amazon.com (US)	Alibaba.com (China); Avito.ru (Russia); Digikala.com (Iran); hepsiburada.com (Turkey)
Whatsapp.com (US)	Wechat.com(China); PTT Messenger (Turkey); Soroush-app.ir (Iran)
Paypal.com (US)	Alipay.com (China); Enpara.com (Turkey)
Uber.com (US)	Didiglobal.com (China); Bitaksi.com (Turkey); Snapp.ir and tap30.ir (Iran)
Booking.com (Holland)	Ctrip.com (China); Tatil.com (Turkey)
Dropbox.com (US)	Disk.yandex.ru (Russia)

Iranian government facilitated the regime by structuring the in- and out-flow of data produced by its citizen users.

As Elinor Ostrom (1990: 202) argues, ‘past institutional choices open up some paths and foreclose others for future institutional development’. Accordingly, our findings reveal how the history of the Iranian nation state, intertwined with nationalist and Islamist discourses, has birthed numerous institutions providing the regime with the opportunities to use the internet as a strategic tool for pacifying the opposition. Particularly, we examine the role of events triggering internet censorship in the 1990s, presenting how they shaped the mentality of policymakers and quality institutions prior to the advent of the digital era in the 2000s. We conclude that the 1990s witnessed a rise in satellite jamming and internet censorship embodied within legal frameworks, creating the prioritisation of security issues over economic objectives.

As cyberspace technology in Iran developed in response to its cyber and propaganda war with Western countries, the Iranian domestic cyberspace came to be shaped at odds with the outside world order. Moreover, internet censorship in Iran suggests that the government maintains concern over both the outflow as well as the inflow of internet data. Our results indicate that nation states such as Iran that maintain strict control of the public and private spheres are inclined to regulate data mobility, defining data to be another public good and therefore to be monitored accordingly. As a consequence, the internet has become a sphere where nation states have invented new methods of collecting, storing, and processing data gathered from the networks of individual users.

Our analysis of the nature and consequences of the regulations in Iran suggests that in parts of the developing world, the planning of the internet economy by nation states plays a significant role in structuring data traffic. This resembles Karl Polanyi’s conception of the formation of a *laissez-faire* economy as described in *The Great Transformation*, wherein he argues that it ‘was the product of deliberate state action, subsequent restrictions on *laissez-faire* started in a spontaneous way’ (Polanyi, 1944 [2001]: 147). Deliberate state movement into the internet economy can operate in multiple ways. For instance, a nation can crowd out the use of global apps through requiring its population to use domestic alternatives (e.g. Yandex or Alipay) on their mobile phones, thereby providing the means for monitoring its citizens.³ As we show below, digital protectionism creates a particular internet ecosystem whereby governments not only apply restrictions, bans, and fines, but likewise employ

³For instance, leaked official documents demonstrate that the Chinese government monitor the daily lives of its citizens, including the Muslim Uyghurs. See the related report at <https://techcrunch.com/2019/11/24/leaked-chinese-government-documents-detail-how-tech-is-used-to-escalate-the-persecution-of-uyghurs/>.

mandates, subsidies, and encouragements. Therefore, we conclude that digital protectionism can function as a form of internet censorship. However, we also think the following clarification should be made:

- (1) digital protectionism is an economic policy of nation states to incentivise domestic companies to operate (more) independently in the internet economy, whereas;
- (2) internet censorship is an undemocratic governmental practice whereby nation states violate the individual's right to obtain information and freely express their thoughts.

There are various studies that address the link between social media penetration and mass mobilisation in democratic and autocratic countries. Using the Egyptian upheaval of 2011 as a case study, Saleh (2012) shows that internet failed to bring freedom to the oppressed society of Egypt and facilitated the consolidation of a military regime. Ananyev *et al.* (2019) examine the role of new information and communication technologies (ICT) in protest coordination and governments' response in the form of content censorship and restricting access to ICTs used for coordination. Qin *et al.* (2017) using China as a case study argue that social media is not only an important tool for content share and social mobilisation; it also provide governments with new opportunities for monitoring activists and local officials. Enikolopov *et al.* (2019a, 2019b) show that the penetration of VK, the largest social networking platform in Russia, increased the probability of the occurrence of social protests while promoting pro-governmental supports.

Other studies focus on the relationship between social media and the quality of democratic institutions. Enikolopov *et al.* (2018) show that 'social media can discipline corruption even in a country with low political competition and heavily censored traditional media'. Acemoglu *et al.* (2018) discuss the role of social media in the Arab Spring. They state that the uprisings in Egypt raised the rents seized by the firms that are politically connected to the government; however, the events did not have significant impact on the firms connected to rival groups. Jha and Kodila-Tedika (2019) argue that there is a positive correlation between democracy and social media penetration especially in low-income countries (see also Kodila-Tedika, 2018.) Reinsberg (2019) argues that 'blockchain technology can enhance the effectiveness and efficiency of foreign aid governance, thereby moving beyond completely anonymous contexts' (see also Davidson *et al.*, 2018). Guriev *et al.* (2019) show that internet penetration does not only cause corruption incidents in the government to expose, it also increases the vote share of populist parties.

Through blocking online transactions and purging global rivals, this study demonstrates how sanctions in Iran contributed to the emergence of domestic start-ups and brands in the internet economy. Brands operate as a kind of capital (Harper and Endres, 2018), and therefore, sanctions and protectionist policies facilitate a sort of capital formation whereby domestic brands function as imitations of their global alternatives. As a result, the Iranian case reveals that an unintended consequence of sanctions on data mobility bear similarities with the intended goals of import substitution digitalisation, in the sense that both favour some sectors of the economy to the detriment of others.

Finally, our study indicates that as a subset of the country's more complex economic and political systems, the digital sector in Iran was incapable of developing either independently of or contradictory to the country's institutional ecosystem. Pagano's notion of interlocking complementarities, borrowed from biology, helps to articulate this last point: various forces within the Iranian nation state taxed or subsidised institutional development in the digital sector, forcing its accordance with the country's founding ideology and economic realities (Pagano, 2011).

2. Censorship in Iran: when motivations define tools

The political order in Iran is based on Islamic-nationalistic narratives exercising severe control over the public and private spheres. Its high oil incomes serve as a crucial resource for facilitating the state's intervention into the economy, culture, and society (Alamdari, 2005: 1285– 1287). The socio-

economic structure of Iran laid the foundations for the establishment of a semi-totalitarian regime, monitoring both data generation and mobility in defence of ‘insiders’ from ‘domestic outsiders’ and foreign rivals (Atwood, 2012). To a significant extent, the 1979 Islamic Revolution was a response to the broadening secular and extravagant lifestyle of an emergent social segment during the 1925–1979 Pahlavi monarchy (Ansari, 1998: 140–146). Institutionally embodying its Islamic ideology, the regime provided a new definition for ‘Iranianness’ founded on a peculiar representation of Shia Islam and its Fars ethnic inner circle. Consequently, the government established an official monopoly on the media and launched the 1980–83 cultural revolution, closing all universities and purging ideological ‘outsider’ students and lecturers, while rewriting books in the humanities and social sciences to replicate the principles of the new ideology (Golkar, 2012: 1–3). While content surveillance in Iran began during the Pahlavi monarchy, it intensified throughout the first decade following the 1979 Islamic Revolution. An exception to this came with the limited liberal reforms for print-publications implemented by the 1997–2005 Khatami government, later reversed to reflect the 2005–2013 Ahmadinejad administration’s Islamic-nationalistic ideology.

During the 2000s, the continuous increase in the number of internet users in Iran was accompanied by pervasive filtering efforts by the government (Aryan *et al.*, 2013a, 2013b). In the 1990s, the strict crackdown on satellite dishes and the filtration of opposition websites resulted in the establishment of domestic channels supplying identical content (Alikhah, 2018). In this period, protectionism was limited to widespread censorship: filtering out the voice of the opposition, defusing the propaganda of rival countries, and according to the official ideology combatting whatever the regime considered detrimental to the ethics and mentality of the people. Internet Service Providers (ISPs) required approval by the government which demanded software implementation to control the contents. Reporters Without Borders reported that prior to 2004, at least 12 ISPs were shut down for not implementing any filtering software.⁴ During this period, the contestation between Iran and the USA surged on the internet, triggering an anti-filter war and cyber-attacks. In 2003, the US government began providing Iranian citizens with free proxies,⁵ followed in 2006 by a \$75 million fund ‘to reach out Iranian people’⁶ alongside \$50 million in 2009 to counter the Iranian government’s efforts to ‘jam radio, satellite, and Internet-based transmissions’ and ‘block, censor, or monitor the internet in Iran’.⁷

Despite the strict filtering policy of the 2000s, blogging became so popular that some service providers ranked among the 10 most popular websites in Iran. People from all levels of society including politicians, activists, and celebrities launched their own blogs (Kelly and Etling, 2008). Following the 2005 blocking of Orkut⁸ some domestic social networks provided services, of which the first and the most important example Cloob⁹ reflected the positive effect of censorship on domestic start-ups in Iran (Hamidi *et al.*, 2011). The manager of Cloob noted that prior to Orkut’s blocking, its number of visitors stood at merely 15,000 members, but following the 2007 filtration its numbers reached 0.4 million. During activation, Cloob developed new services, including Coroob, an inter-user transferable virtual currency enabling members to buy services such as the ability to conduct advanced searches in contents, bookkeeping, or see a list of profile visitors.¹⁰

Ahmadinejad’s controversial declaration of victory in the 2009 presidential election triggered a series of mass uprisings (Karagiannopoulos, 2012: 153–157). Users shared censored news of unrest and videos of violent oppression via Facebook and Twitter, while Farsi satellite TV channels widely covered

⁴https://web.archive.org/web/20080224063811/http://www.rsf.org/article.php?id_article=10733.

⁵https://www.theregister.co.uk/2003/08/29/us_sponsors_anonymiser_if_you/.

⁶<https://www.washingtoninstitute.org/policy-analysis/view/u.s.-support-for-the-iranian-opposition>.

⁷<https://www.casey.senate.gov/newsroom/releases/senate-adopts-victims-of-iranian-censorship-voice-act>.

⁸Orkut was a social networking website designed by a Google employee to help internet users to meet new and old friends. It was shut down in 2014. For more details see Kumar *et al.* (2012).

⁹Cloob is a Farsi-language domestic social network for sharing content with other users and meeting new friends. Its online web address is: <https://www.cloob.com/>. See also Naghibulsadat *et al.* (2015) for a comparative study of contents preferred by Iranian users using both domestic (including Cloob) and non-Iranian social networks.

¹⁰<http://bit.ly/2KRE60E>.

the events. In response, the regime filtered social networks and restricted internet bandwidth, in addition to using terrestrial jamming methods to interrupt the connection between private dishes and the satellite TV channels now officially determined illegal (Baldino and Goold, 2014; Rahimi, 2011). A survey conducted by the Iranian Student Polling Agency (ISPA) indicates that censorship not only led to a decrease in satellite channel viewers but likewise decreased general trust in official media, a phenomenon replicated by falling numbers in official radio and TV viewers.¹¹ The regime's reaction to the 2009 presidential unrest provides evidence demonstrating that restrictions in data traffic are frequently contingent upon unpredictable events. Consequently, such interventionist policies generated the environment for the emergence of domestic alternatives.

The aftermath of the 2009 presidential elections culminated in the peak of censorship, filtering, satellite jamming, and the VPN war. Documents subsequently released by WikiLeaks detailed further acts of digital espionage conducted against Iran (Farwell and Rohozinski, 2011; Pieterse, 2012). An Israeli-American made malicious computer worm named Stuxnet attacked the Programmable Logic Controller (PLC) and the Supervisory Control and Data Acquisition (SCADA) operating Iran's uranium enrichment systems, resulting in substantial damages to the country's nuclear programme (Farwell and Rohozinski, 2011; Lindsay, 2013). In the autumn of 2009, Twitter suffered global disruption. In 2011, a number of American banks and the computer system of a reservoir dam suffered attacks by hackers; in the same year, a virus called Shamoon hit the Qatari and Saudi state-run gas and oil companies. And in 2012, the International Atomic Energy Agency's servers were hacked. Although Iran never accepted responsibility for these cyber-attacks, they were attributed to the Iranian Cyber Army (Bronk, and Tikk-Ringas, 2013; Farwell and Arakelian, 2013; Guitton and Korzak, 2013; Kenney, 2015; Rid and Buchanan, 2015). These cyber-attacks are indicative of the Iranian nation state developing new capacities for intervention into the communicative transactions of the internet (Al-Rawi, 2014; Berman, 2013; Craig and Valeriano, 2016).

The formation of the Iranian Cyber Army and the development of required technologies reveal a causal relationship between the non-economic rules of the game and the evolution of institutions and organisations. Some sources rank the Iranian Cyber Army among the top five in the world,¹² on account of the country's capacity to meet its large domestic demand for required software.¹³ However, there are general doubts as to its ability to compete internationally. Israeli sources claim that in terms of cyber-warfare capabilities, Iran is considered to be on a par with the most advanced countries, stressing its ability to launch cyber-attacks in the case of war against Western nations' energy infrastructures, transportation systems, and financial institutions.¹⁴ Although several sources concede the country's ability to supply advanced software, their illegal application combined with the reaction of their target countries hinders Iran's potential to benefit economically from its technology's market advantages.

3. National Information Network

The Stuxnet experience alerted the Iranian regime as to the potential for the disastrous effects of a future widespread cyber-attack. Such an event might target its principal political and economic centres, including its nuclear plants, ministries, infrastructures, official media, and banks. As a result, the original concept of establishing a 'halal internet' providing content according to the regime's Islamic narratives evolved into a national security project. Started during Ahmadinejad's presidency, this was supposed to operate as an intranet network for contacting vital centres. It was initially branded the

¹¹<http://bit.ly/2zlhGOQ>.

¹²<https://www.hackread.com/iran-biggest-cyber-army-israel/>.

¹³According to a report published by DefenseTech, as of 2008, Iran's software output was valued at about \$50 million and its cyber warfare budget at \$76 million. See <https://www.military.com/defensetech/2008/09/23/iranian-cyber-warfare-threat-assessment>.

¹⁴<https://www.hackread.com/iran-biggest-cyber-army-israel> and <https://www.slideshare.net/HackRead/irans-cyber-war-skills>.

National Internet, but after some amendments, the Supreme Council of Cyberspace (SCC) retitled it as National Information Network (NIN) (Rahimi, 2015). The definition and requirements of the NIN were approved in 2013, with the Ministry of Information and Communications Technology determined its project executive. The SCC hailed the NIN one of its most important national cyberspace projects and the communicational framework of the country's cyberspace.¹⁵ The subsequent law enacted as of 2016 specified that the realisation of this project demanded compliance with such national requirements as providing advanced infrastructural services matching the country's necessities, the utilisation of the economic advantages of national cyberspace industry, the protection and development of Irani-Islamic culture in cyberspace, and security regarding Iranian users' private information against external threats. The NIN was defined as a network based on the internet protocol, comprising switches, routers, and data centres, allowing or denying internal access requests to receive information maintained in its domestic data centres. Additionally, the NIN hinders the potential for tracing from abroad and provides a secure and private intranet network.¹⁶

Initially, the focus of the NIN project fell on non-economic security issues on the internet. Breaking tradition with Iran's tendency towards reactionary responses, collaborating units within the regime designed a strategic project intended for long-term usage. Crucially, the project clearly defined its institutions and legal frameworks, and so we can characterise the NIN's targets into two main alignments. Firstly, to minimise security concerns by providing a network independent of the internet, facilitating controlled cooperation with other networks, and solidifying safe and sustainable communication between the country's different core organisations. Secondly, to meet the criteria demanded by the domestic market by supplying diverse content, country-wide services, wide bandwidth, a data centre, and internal hosting at a competitive price.¹⁷ Statements by Saidreza Ameli, the Secretary of the Supreme Council of the Cultural Revolution, clarify the scope of the project and funding; in May 2019, he declared 80% progress in the NIN project, maintaining that 12,000 billion Tomans from the public budget and 7,000 billion Tomans in private funds had been allocated for developing the NIN's infrastructure.¹⁸

Despite various attempts to emphasise the prerequisites for creating a highly competitive network, the NIN's complementary 2017 decision required lower prices for data trafficking compared to the global internet. This discount was suggested to amount to 50% for all consumers and 90% for 'qualified' units and users.¹⁹ Initially, this may appear a short-term policy supporting the NIN by encouraging users and institutions to choose the domestic alternative, but this practice resembles similar traps that have previously ensnared state-run parastatals, such as factories and banks. For instance, complete nationalisation of the financial system due to similar ideological concerns relating to the dominance of non-Islamic-Irani rules in banking system resulted in its subsequent lack of profitability. Accordingly, a phenomenon called 'banking dilemma' emerged out of the long-term non-profitability, despite no significant report of bankruptcy in the system. The 'banking dilemma' demonstrates the existence of widespread rent-seeking within the financial system, and the reality of public resources being used for the benefit of the banks (Karamelikli and Alizadeh, 2017: 56).²⁰

¹⁵The Supreme Council of Cyberspace (2013 and 2016) Outline for the National Information Network is available at: http://www.majazi.ir/parameters/majazi/modules/cdk/upload/content/general_content/849/1509970008746mjnk60snusgb-qu9diuete92ld0.pdf, p. 2.

¹⁶Ibid., p. 3.

¹⁷Ibid., pp. 3–9.

¹⁸Although there are shortcomings in the exact details of the realised budgets for each year, by grouping different information together and taking the official exchange rate as a basis, up to 2019, it seems at least \$4 billion have been invested in infrastructures of NIN: <http://bit.ly/2Zgvtpd>.

¹⁹<http://www.tct.ir/uploads/251-1.pdf>.

²⁰Four decades after the establishment of an Islamic-banking system in Iran and the lock-in phenomenon in Iranian banks, those sectors intertwined with the banking system and their 'insiders' resist the enforcement of any criteria which may prepare them to compete internationally (Alizadeh, 2019: 35–41).

Doubts as to the NIN's competitive capability have increased as no deadline established for internet subsidisation. More importantly, the government have deliberately restricted internet speed and filtered millions of sites. Currently, it is evident that the domestic digital networks and the available manufactured content therein have assumed the features of the artificial state-made environment, and therefore, do not possess the qualities necessary for surviving competitive conditions. Hence, in the same line with Pagano's 'interlocking complementarities' notion, when a significant share of cyber activities transfers to the NIN, its entrance into the global market may prove much harder because of friction with its established institutions. In other words, the beneficiaries of rent and employment opportunities provided by the state-led development in the NIN can be resistant to the market-oriented reforms.

4. Sanctions: restriction or opportunity?

The Iranian economy is well known for its high dependence on oil incomes; however, ongoing economic crises and temporary stabilities have been another feature of the economy. The 8-year Iran–Iraq war, political turmoil, fluctuations in oil incomes and exchange rates, alongside high inflation rates, and several international sanctions have remained the reality of Iran for over four decades. During the Ahmadinejad era (2005–2013), sanctions escalated in relation to the country's nuclear programme, hitting the roof in 2010 after the introduction of comprehensive sanctions led by the USA, the UN, and the EU. Sanctions blocked the links of Iranian banks to international networks, alongside hindering the online transactions of the Iranian people (Arnold, 2016: 85). Consequently, while for many countries, digital protectionism may serve as one among many possible economic choices, in Iran it became an inescapable inevitability as sanctions imposed barriers on data transfer.

Sanctions set the foundation for the emergence and development of new domestic digital service providers in Iran. One of the founders of Digikala, the Iranian equivalent of Amazon, confirms that sanctions created an opportunity for many start-ups to begin their own businesses and be prepared for the time when large international companies entered the market (Salamzadeh and Kesim, 2017: 465). In the summer of 2019, Alexa ranked Digikala as the third most visited site in Iran and the most visited online store in the Middle East. By comparison, another Iranian e-commerce marketplace start-up named Bamilo had a less fortunate lifecycle. As one of the largest ventures of the Iran Internet Group (IIG) and backed by South African multinational corporation MTN, Bamilo hoped to usher in a new era of international investment in the Iranian market but instead wound up defunct as of March 2019.

However, not all domestic start-ups fared as poorly as Bamilo. Ranked by Alexa as the 9th, 39th, and 47th most visited websites of 2019, Divar, Sheypoor, and Emalls are online marketplaces with Android applications for new and second-hand goods, renting, advertising, and services. Esam, an Iranian equivalent of eBay, is an auction and shopping website facilitating business–consumer and consumer–consumer online sales. Takhfifan, the domestic version of Groupon, is an e-commerce platform providing discounts for group purchases. The Megagroup and Iranecar portals provide services in the automotive sector for selling and buying domestic and imported cars, accessories, and spare parts, alongside services such as leasing and insurance. Raja and Cinematicket are examples of websites that sell train and cinema tickets, respectively. Cafe Bazar and Myket are two Iranian versions of the Google Play app store. With about 400 million USD assets and 40 million users, Cafe Bazar is an Android marketplace providing different domestic and international applications.²¹ There are reports indicating that because of language similarities, this app and its online services extend as far as Afghanistan.²²

Despite the strict controls on fashion-related businesses to curtail the potential to imitate Western lifestyles, websites such as Modiseh and Shexon managed to develop services focusing on stylish

²¹<https://financialtribune.com/articles/sci-tech/97365/iranian-android-market-records-40-million-active-users>.

²²<http://techrasa.com/2016/08/23/cafe-bazaar-divar-expand-afghanistan/>.

products. Likewise, there are apps such as Boghche offering different traditional Iranian bakery products, Reyhoon for the online ordering of food, and MamanPaz for delivering home-made food cooked by housewives in an app user's vicinity. Shafajoo, the Iranian equivalent of Doctena, is a healthcare platform providing services such as doctor appointments and online counselling courses. Likewise, Alexa ranked the website of Shaparak, the Central Bank of Iran's electronic card payment system founded for the centralisation and reorganisation of the points of sale (POSS), as the sixth most visited website in Iran in the summer of 2019. Snapp, supported by the Iran Internet Group and MTN Group, alongside Tap30, are Iranian versions of Uber, and rank the two most popular ride-hailing platforms providing services via Android and the web. Additionally, there are domestic hotel, ticket, and tourist trip booking websites ranked among the 200–500 most visited Iranian websites of 2019.

A number of sites, including SID, Magiran, and Noormag, host articles published in Iranian academic journals, while the Ensani website provides articles from Iranian journals of the humanities and social science. Alongside a lack of legal mechanisms necessary to control copyright, the sanction-induced international payment barriers affected the printing sector in two ways: firstly, the institution's condition contributed to the development of the illegal translation and publication of unavailable books. Secondly, it gave momentum to the emergence of several free download websites; Fardabook, Fidibo, Ketabnak, Takbook, TXT, and Ketabesabz among others provide a vast number of books for free download, while various websites sell student's homework, presentation files, and even theses, alongside illegally downloaded books in a multitude of languages.

As a result of the filtering of YouTube for the purpose of censoring 'immoral' and anti-regime content (Golkar, 2011: 58–60), in the summer of 2019, Iranian video sharing services such as Aparat, Didestan, and Dalfak respectively ranked the 2nd, 33rd, and 41st most visited domestic websites. Similarly taking advantage of this and the crackdown on satellite dishes, Telewebion, Film2Movie, Mydiba, and Filmo entered the list of the 50 websites most visited by Iranians by providing services for downloading films and live streaming officially-sanctioned television programmes. Hamijoo, an Iranian version of Indiegogo, is an online crowdfunder launched to raise money for projects including art and film. Additionally, the Iranian Central Bank began supporting fintech projects to make Iran the financial hub of the Middle East.²³ ZarinPal, YekPay, PayPing, and Bahamta are Iranian alternatives to PayPal, developed to solve online payment problems primarily induced by sanctions. Mehrabane is another crowdfunding platform aimed at raising funds for deprived people, patients, education, and health issues.

Despite these opportunities, sanctions created difficulties for finding foreign investors and transferring money (Safshekan, 2017). Although many start-ups may owe their successes to governmental support, finding proper investors has become a significant problem for business owners setting up new companies in the digital market (Salamzadeh and Kesim, 2017: 469–470). These financing problems present new opportunities for start-up accelerators. For instance, Iran Fara Bourse has founded an over-the-counter initiative to address the initial public offering problem. Moreover, start-up accelerators such as Avatech, Dmond, TrigUp, MAPS, Setak, and Finnova, along with venture capital firms such as Sarava, Shenasa, and the IRATEL venture, emerged to fill the gap in the domestic start-up ecosystem (Ismail *et al.*, 2018; Kanani and Goodarzi, 2017; Lalmohammadi, 2016; Sammaknejad, 2017). Finally, professional start-up media including Techrasa, Shanbemag, Dr.startup, and Khoshfekri, among others, aim to share and develop a network of Iranian entrepreneurs via magazines, tutorial products, and news.

5. New frontiers in cyber-war: social networks and Android messenger apps

In 2013, President Rouhani's electoral platform focused on solving nuclear problems and opening the Iranian economy to the world market. To attract younger voters, he also talked about the necessity of

²³<http://fintechnews.ch/fintech/fintech-iran-overview/11423>.

freedom in society, but the following course of events revealed that regime hardliners and unpredictable events were able to overpower any sincerity in these sentiments. As mentioned previously, social networks such as YouTube had been censored prior to the 2009 presidential election, with Facebook and Twitter suffering a similar fate after the resulting election unrest later that year. An increase in mobile phone internet connectivity and the popularity of Android apps generated a number of recent changes (Alimardani and Milan, 2018; Kazanin, 2017). Viber was among the first apps to be popular among Iranians, and in 2015, accounting for 18% of all users, Iranians were the leading group of Viber users in the world (Khiabany, 2018: 228). Since 2015, Telegram users have rapidly surged, with the app in turn growing into the most popular social network app among the Iranian public (Alimardani and Milan, 2018). Statistics of a survey conducted by the ISPA indicate that in 2015, 38% of its respondents were using Telegram and 17% were using WhatsApp.²⁴ Firouzabadi, the Secretary of the Supreme Council in Cyberspace, admitted that in 2016, Telegram and WhatsApp users totalled 24 and 12–14 million, respectively.²⁵ ISPA's 2017 survey revealed that 55% of its respondents were using the Telegram app, while 23% of the sample used Instagram, alongside WhatsApp (14%), Facebook (4%), Viber (2%), Google+ (2%), and Twitter (1%). The study depicted 5% of its respondents using the internet to watch pornography, whereas 69.3% used VPNs and other anti-filter programs for visiting censored websites.²⁶ A survey conducted by two online research websites in the same year presents less than 5% of respondents using domestic social networks such as Cloob and Soroush.²⁷

Iran's nuclear deal – known as the Joint Comprehensive Plan of Action (JCPA) – initially appeared promising for the economy; however, having experienced a 1-year boom in the oil sector, 2017 saw the economy entering another period of stagnation. In the United States, the presidency of Donald Trump and his promise for withdrawal from the JCPA caused strict instabilities in the Iranian economy, to the extent that in 2018, inflation and foreign exchange rates increased over two and three times. January 2018 witnessed harsh unrest in small cities, with Telegram utilised for mobilising protestors and sharing news. In the USA, these events encouraged President Trump, Secretary of State Mike Pompeo, and National Security Advisor John Bolton to support protestors with the intention of pressuring the regime. Likewise, they requested Google, Facebook, and other social networks provide protestors with extra communication facilities.²⁸ Owing to security reasons, in May 2018 the regime blocked Telegram; however, despite heated debates about the effectiveness of internet filtering, Instagram and WhatsApp are currently tolerated. While hardliners supported the policy, President Rouhani and Jahromi, the Minister of Information and Communication Technology, termed it futile. Recalling the ineffective bans on radio during the first decade of the Islamic Revolution, Rouhani declared the censorship policy to be pointless. He also invited hardliners to propose a cultural solution for securing cyberspace.²⁹ Once again security concerns, such as the mobilisation of protestors and the transfer of user data across the borders, proved the catalyst for internet filtering rather than economic motivations. However, this time the regime offered domestic alternatives, such as the Soroush app.

Numerous surveys demonstrate that the first 6 months after Telegram's blocking instigated an increase in the market share of its domestic alternatives; however, these intervention-induced trends were to reversed 6 months later. ISPA's survey depicts 60% of its respondents using Telegram in March 2018, but by June the number of users dropped to 50%, and fell further in October to 47%, before rising again in March 2019 to reach 56%. During the period between March 2018 and March 2019, Instagram and WhatsApp users doubled, reaching 30 and 25%, respectively. The statistics for the Soroush domestic app appeared initially promising, before declining in the following months. The same survey presents Soroush's visitors increasing from 2 to 14% in less than 3 months after the

²⁴<http://bit.ly/2ZjsxDm>.

²⁵<http://bit.ly/33PF3xQ>.

²⁶<http://bit.ly/2KS2WgG>.

²⁷<http://bit.ly/2ZhOHeb>.

²⁸<https://www.independent.co.uk/news/world/middle-east/iran-halal-internet-national-information-network-web-free-dom-citizens-access-social-media-telegram-a8182841.html>.

²⁹*ibid.*

internet filtration, before declining to 4% in October 2018 and 2% in March 2019. Statistics for other domestic social networks such as Baleh, ITA, Gap, and IGap conform to this trend.³⁰ Furthermore, Facenema, an Iranian alternative for Facebook, proved unsuccessful in attracting users.³¹ Considering its 5 billion Tomans credit³² and half-price internet facilities, it appears Rouhani and Jahromi were at least correct in the short-term in describing internet filtering as a futile policy.

A consequence of the ban on Telegram became the widespread use of anti-filters, unofficial versions of Telegram, and an increase in the users of unfiltered social networks such as Instagram and WhatsApp, presently labouring under a similar threat of blocking. In June 2018, Khorramabadi and Javadnia, the former and new Vice Attorney General in Cyberspace Affairs maintained that 30–35 million Iranians were using 127 imitation versions of Telegram, including Hotgram and Talagram, to contact the main server.³³ Khorramabadi termed these client versions anti-filter, but debates about these apps became heated after they subsequently blocked channels such as BBC Persian.³⁴ By comparison, some of the deputies and intelligence service officials proclaimed the Talagram client to be legal, belonging to the Islamic Republic of Iran and possessing 25 million users. Firouzabadi, the Head of National Cyberspace, also admitted Hotgram and Talagram were domestic imitations of Telegram. The regime would tolerate these versions until the future launch of a 100% domestic app. Nazemi, the Head of Information Technologies Institutes, claimed that for 2 years the FAVA research institute, a state-run firm for the development of communication and information, had been designing a new domestic operating system to strengthen the capacity for Iranian resilience in the face of the US's economic terrorism. Additionally, BBC Persian reported claims regarding the import of 2,000 servers for Hotgram and Talagram, alongside subsidised exchange rates.³⁵

Filtering and the access of the Iranian government to the 'identity verification codes' of Iranian users prompted the Human Rights Commission of Iran to caution as to the security of fake versions of Telegram.³⁶ Consequently, in April 2019, Google removed Talagram and Hotgram from the Google Play store for reasons of espionage and the theft of its users' personal data.³⁷ In 2019, YouTube, Twitter, Facebook, and Instagram blocked the accounts of some of the top-ranking officials of Iran, heralding a new phase in cyber warfare.³⁸ As internet restriction turns into a worldwide phenomenon, blocking is now the recourse of even former advocates of freedom of information.

Rising gasoline prices in November 2019 triggered one of the most violent demonstrations of the last 40 years, with hundreds³⁹ of lives lost and serious damage to 731 banks, 70 gasoline stations, and about 2,000 motor vehicles. Instead of restricting internet bandwidth or adopting censorship in retaliation, the government took an unprecedented decision to unplug the internet connection in order to

³⁰<http://bit.ly/33YPnnq>.

³¹For instance, during the first half of 2019, Facenema was among the 150–200 most visited websites in Iran.

³²<https://bit.ly/2MApMM1>.

³³<http://bit.ly/30sx2ge>.

³⁴<http://www.bbc.com/persian/blog-viewpoints-48093652>.

³⁵Ibid.

³⁶<https://iranhumanrights.org/2018/12/why-did-telegram-warn-users-that-iranian-versions-of-app-telegram-talaeii-and-hotgram-are-unsafe/>.

³⁷<https://en.radiofarda.com/a/lawmaker-says-iran-behind-bogus-messaging-apps-banned-by-google/29924990.html>.

³⁸<https://www.engadget.com/2019/06/13/twitter-removes-iran-accounts/>.

<https://www.france24.com/en/20190416-instagram-accounts-iran-guards-commanders-blocked>.

<https://www.rferl.org/a/instant-ban-for-iran-s-irgc-on-instagram-social-media-giant-blocks-commanders-sites/29886908.html>.

³⁹According to a report by Amnesty International released on 16th December 2019, at least 304 people were killed and thousands were arrested during these unrests. However, Reuters reports about 1,500 lives lost including at least 17 teenagers and about 400 women, alongside some members of the security forces and police. See <https://www.amnesty.org/en/latest/news/2019/12/iran-thousands-arbitrarily-detained-and-at-risk-of-torture-in-chilling-post-protest-crackdown/> and <https://www.reuters.com/article/us-iran-protests-specialreport/special-report-irans-leader-ordered-crackdown-on-unrest-do-what-ever-it-takes-to-end-it-idUSKBN1YR0QR>.

control social networks and block the information leak to the media. Although the internet blackout caused 2,950 billion Toman damages in the first 10 days owing to the considerable decline in online marketing, banking, start-ups' payment transactions, and the services of telephone operators,⁴⁰ those websites on the NIN and domestic messaging apps were permitted to continue their services.⁴¹ The event inevitably animated the debate among proponents and opponents of the NIN. Jahromi, the Minister of Information and Communication Technology, maintained that thanks to the NIN, 2.5 million people employed by online mobility service providers avoided joining the protesters in the streets.⁴² President Rouhani maintained that the Supreme Leader asked the government to develop the NIN to sever the Iranian peoples' dependence on foreign corporations.⁴³

Although censorship has evolved to address the security-ideological concerns of the regime and its 'insiders', it has similarly adversely affected the social capital of Iranian society through the formation of state-induced 'filter bubbles'. Different studies suggest that in the wake of official propaganda, those maintaining an ideological affinity to the regime alongside the more apolitical but pious segments of Iranian society perceive officially unadmitted internet channels as a tool of anti-regime or anti-Islam propaganda.⁴⁴ As a result, these parts of the society voluntarily abstain from or avoid access to any censored social media or internet, instead consuming content produced by the official media. By comparison, opponents of the regime have lost trust in the officially sanctioned media and consume censored television content. Therefore, like-minded segments have clustered around the opposite ends of the spectrum, with each developing their own 'echo chamber' and 'confirmation bias'. The repetition of specific ideas inside a closed system invariably foreshadows the formation of cultural tribalism, with a lack of alternatives producing a 'tunnel vision' phenomenon. The result is the formation of faction-based conflicts, creating social damage and destroying social capital within society.

6. Conclusion

The fears and motivations of political authorities determine the tools and methods adopted for monitoring and protecting international data transfers. For Iran, the ideological structure of the regime, the economic structure of the country, and the historical contingencies of the nation have significantly affected the scope and quality of protectionist policies. Prior to 2010, events posing risk to the security of the regime were among the key factors influencing the implementation of protectionist policies in the form of censorship. The regime's beliefs regarding the significance of nationalistic-Islamic ideology in maintaining national security resulted in the widespread surveillance of data and information transfer in both the public and private spheres. Since 2010, three factors have changed the regime's perspective on digital protectionism. Firstly, the increased penetration of the internet into Iranian society and the popularity of social media amplified the role of digital media in generating social mobilisation. Secondly, cyber-attacks executed by rival countries developed into a tangible threat, with the regime

⁴⁰With market and official exchange rates, damages from the internet blackout amount to 2.5 and 7.5 billion dollars, respectively. See the report by Iran's Chamber of Commerce, Industries, Mines, and Agriculture at <https://bit.ly/2s6E3ar>.

⁴¹<https://www.atlanticcouncil.org/blogs/iransource/iranians-endure-internet-shutdown-with-despair-and-disarray/>.

⁴²<https://bit.ly/2sfybeL>.

⁴³<https://www.youtube.com/watch?v=JFN-6ao0M1o>.

⁴⁴A study conducted by the Iranian Police refers to the formation of pious user networks on social media that retain intra-group solidarity. The study maintains that these groups are connected with law enforcement, and self-police the contents of the community (Habibzadeh and Bakhshi, 2016). Another police study states that social networks are directly responsible for creating social crisis in Tehran (Mohammadi *et al.*, 2017). Ziaieparvar (2009) maintains that 'regime enemies' use social networks such as Facebook and YouTube in a soft cyber war against Iran. These studies imply that in the eyes of police at least, users of social media are divided into 'insiders' as trustful users and 'others' who use filtered social media in officially inadmissible ways. Moreover, there are various studies attempting to examine the effect of social networks on the family institution (Fallahi, 2016; Hosseinpour and Momeni, 2017), infidelity (Seyyedalitabar *et al.*, 2015), impiety and religious identity (Kian and Qolipour, 2016; Mirfardi *et al.*, 2017; Qasemi *et al.*, 2013; Rostami *et al.*, 2017; Sharifi and Shahrestani, 2017), national identity (Salavatian and Dovlatkhah, 2017), identity crises (Memar *et al.*, 2012), immorality (Sharafaddin and Eqbali, 2016), and foreign malicious penetration projects (Fouladi and Banakar, 2017; Razavi *et al.*, 2018).

likewise coming to understand its potential for use in retaliation. Thirdly, continuous increases in the ratio of ICT added-value to GDP as a global trend (Moshiri *et al.*, 2018; Nasab and Aghaei, 2009) proved the importance of government intervention into the internet economy,⁴⁵ signalling new rent-seeking opportunities for its ‘insiders’.

The case of Iran indicates that digital protectionist policies are unable to substantially accomplish pre-determined goals in the presence of methods for circumventing the barriers. However, digital protectionism causes the costs of transactions to rise when accessing blocked websites. In the targeted countries, sanctions are powerful tools for restricting a citizen’s access to the digitised world market. The barriers imposed by protectionist policies and sanctions hinder competition, and consequently, provide domestic start-ups with an empty playing field. However, the example of Iran suggests digital protectionism may cause additional difficulties in terms of funding and technology transfer.

We can define start-ups as new-born companies or ventures attempting to practice original ideas in the marketplace. By comparison, Iran’s domestic alternatives are merely copies of larger corporations such as YouTube, Amazon, and WhatsApp. The lifecycle of these domestic alternatives proves that they have managed to receive some of the added value produced by the domestic digital market. By accounting for the effects of sanctions alongside that of protectionist policies, these emerging domestic start-ups have partially succeeded to substitute import services by their duplicated counterparts.

It is evident that some ‘insiders’ happen to be the beneficiaries of Iran’s digital protectionist policies. But the remainder of society has to make decisions regarding the transaction costs of accessing the higher quality goods and services available on the internet compared to their lower quality domestic alternatives. Furthermore, with or without protectionist policies, citizens hold little control over their own personal data, as rather than preventing its monitoring, the sole function of Iran’s policies is to permit the regime’s domestic or international firms to control massive amounts of user data. As a result, even by accepting the propositions of data colonialism, digital protectionism facilitates a form of internal data colonialism supplanting the external one.

In most cases, the policies of digital protectionism lack a coherent strategy because the government appears to neglect any form of macro plan. Its policies can lack long-term perspective and often disregard the role of all the players in the game. Except for the NIN project and the cyberspace topics in Iran’s Sixth Development Plan (2016–2021), protectionist policies lacked support underscored by proper funding strategies. Its policies of digital protectionism have mostly remained contingent on unexpected events and evolved according to these circumstances, with related institutions formed for handling these anomalies. In many cases, protectionist policies failed to produce their predicted results due to shortcomings in providing high quality alternatives and the existence of different circumvention methods such as VPNs.

In Iran, such policy centres as the Supreme Council of Cyberspace and the Ministry of Information and Communications Technology hold responsibility for censorship and cyberspace surveillance. These centres have developed sophisticated technologies, recruited experienced staff, and established one of the best cyber armies in the world to protect domestic networks. In the future, these skills and technologies may come to positively influence other sectors of the Iranian economy; however, the illegal character of the government’s intervention on the web is a significant barrier to their domestic and international commercialisation. Experiences from state-run factories and banks show that interventionist policies can initially cause tremendous changes in the conditions of the economy, clustering different economic and political activities around the subsidised sector, but eventually suffer through locking the economy, polity, and society on an unproductive future path.

⁴⁵While the ICT market witnessed approximately 2% annual growth during the 2000s, this trend sharply increased in the 2010s. According to Jahromi, Rouhani’s Minister of Information and Communication Technology, between 2013 and 2017, the ICT market jumped from 19,000 billion Tomans to 40,000 billion Tomans, with the official exchange rate amounting to 12 billion USD. See <https://bit.ly/2sfybeL>.

Acknowledgement. An earlier version of this paper was presented at the International Conference of TED University Trade Center (TRC), Ankara, 13–14 June 2019 and the 16th Italian Association for the History of Political Economy (STOREP) Annual Conference, Siena, 27–29 June 2019. We would like to thank Stefano Lucarelli, Christian Fuchs, Geoffrey Hodgson, Katie Blythe, and the anonymous referees of this journal for their helpful remarks. Remaining errors are ours.

References

- Pagano, U. (2011), 'Interlocking Complementarities and Institutional Change', *Journal of Institutional Economics*, 7(3): 373–392.
- Fouladi, M. and R. Banakar (2017), 'Shiveha va Shegerdhave Nofuze Ejtemai Farhangi', *Maarefate Farhangi Ejtemai*, 8(2):55–80.
- Aaranson, A. S. (2018), 'What are We Talking About When We Talk About Digital Protectionism', *World Trade Review*, 18 (4): 541–577.
- Aaronson, S. A. (2016a), 'The Digital Trade Imbalance and Its Implications for Internet Governance', Centre for International Governance Innovation, No. 25 February, http://www.cigionline.org/sites/default/files/gcig_no25_web_0.pdf (accessed 21 October 2019).
- Aaronson, S. A. (2016b), 'Digital Protectionism? Or Label the US Government Uses to Criticize Policy It Doesn't Like?', Council on Foreign Relations, March 3, <http://www.cfr.org/blog-post/digital-protectionism-or-label-us-government-uses-criticize-policy-it-doesnt> (accessed 21 October 2019).
- Acemoglu, D., A. H. Tarek and A. Tahoun (2018), 'The Power of the Street: Evidence from Egypt's Arab Spring', *Review of Financial Studies, Society for Financial Studies*, 31(1): 1–42.
- Ahmad, J. (1978), *Import Substitution, Trade, and Development*, Greenwich, Connecticut: JAI Press.
- Al-Rawi, A. K. (2014), 'Cyber Warriors in the Middle East: The Case of the Syrian Electronic Army', *Public Relations Review*, 40(3): 420–428.
- Alamdari, K. (2005), 'The Power Structure of the Islamic Republic of Iran: Transition from Populism to Clientelism, and Militarization of the Government', *Third World Quarterly*, 26(8): 1285–1301.
- Alikhah, F. (2018), 'A Brief History of the Development of Satellite Channels in Iran', *Global Media and Communication*, 14(1): 3–29.
- Alimardani, M. and S. Milan (2018), 'The Internet as a Global/Local Site of Contestation: The Case of Iran', in E. Peeren, R. Celikates, J. Kloet and T. Poell (eds.), *Global Cultures of Contestation*, Cham: Palgrave, Macmillan, pp. 171–192.
- Alizadeh, N. (2019), 'Ekonomik Direnc ve Kırılgnalık: İran'da Bankacılık Sistemi', *Bankacılık ve Sigortacılık Araştırmaları Dergisi*, 5(13): 33–43.
- Ananyev, M., D. Xefteris, G. Zudenkova and M. Petrova (2019), 'Information and Communication Technologies, Protests, and Censorship'. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2978549 (accessed 10 February 2020).
- Ansari, A. M. (1998), *Shah Mohammad Reza Pahlavi and the Myth of Imperial Authority*, Doctoral dissertation, SOAS University of London.
- Arnold, A. (2016), 'The True Costs of Financial Sanctions', *Survival*, 58(3): 77–100.
- Aryan, S., H. Aryan and J. A. Halderman (2013a), *Free and Open Communications on the Internet*, Washington, DC: USENIX Association.
- Aryan, S., H. Aryan and J. A. Halderman (2013b), 'Internet Censorship in Iran: A First Look', in *Presented as part of the 3rd Workshop on Free and Open Communications on the Internet*.
- Atwood, B. (2012), 'Sense and Censorship in the Islamic Republic of Iran', *World Literature Today*, 86(3): 38–41.
- Baer, W. (1972), 'Import Substitution and Industrialization in Latin America: Experience and Interpretation', *Latin American Research Review*, 71(1): 95–122.
- Baldino, D. and J. Goold (2014), 'Iran and the Emergence of Information and Communications Technology: The Evolution of Revolution?', *Australian Journal of International Affairs*, 68(1): 17–35.
- Berman, I. (2013), 'The Iranian Cyber Threat, Revisited', Statement Before the US House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, 2.
- Bronk, C. and E. Tikk-Ringas (2013), 'The Cyber Attack on Saudi Aramco', *Survival*, 55(2): 81–96.
- Bulut, E. (2016), 'Social Media and the Nation State: Of Revolution and Collaboration', *Media, Culture, and Society*, 38(4): 606–618.
- Calder, S. (2017), 'Turkey has Banned Booking.com But the Website isn't Backing Down', *The Independent*. <https://www.independent.co.uk/travel/news-and-advice/bookingcom-turkey-priceline-hotels-court-istanbul-ankara-ban-competition-authority-a7658251.html> (accessed 21 October 2019).
- Chang, H. J. (2002), *Kicking Away the Ladder: Development Strategy in Historical Perspective*, London: Anthem Press.
- Cockcroft, J. D., A. G. Frank and D. L. Johnson (1972), *Dependence and Underdevelopment and Underdevelopment: Latin America's Political Economy*, New York: Anchor Books.
- Craig, A. and B. Valeriano (2016), 'Conceptualising Cyber Arms Races', In *8th International Conference on Cyber Conflict (CyCon)*, IEEE, pp. 141–158.

- Davidson, S., P. De Filippi and J. Potts (2018), 'Blockchains and the Economic Institutions of Capitalism', *Journal of Institutional Economics*, **14**(4): 639–658.
- DeNardis, L. (2014), *The Global War for Internet Governance*, New Haven and London: Yale University Press.
- Enikolopov, R., A. Makarin and M. Petrova (2019a), 'Social Media and Protest Participation: Evidence from Russia', https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2696236 (accessed 10 February 2020).
- Enikolopov, R., M. Petrova and K. Sonin (2018), 'Social Media and Corruption', *American Economic Journal: Applied Economics*, **10**(1): 150–174.
- Enikolopov, R., M. Petrova and E. Zhuravskaya (2019b), 'Political Effects of the Internet and Social Media', CEPR Discussion Papers 13996, C.E.P.R. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3439957 (accessed 10 February 2020).
- Everard, J. (2000), *Virtual States: The Internet and the Boundaries of the Nation-State*, London and New York: Routledge.
- Fallahi, A. (2016), 'Tahlile Keyfi va Kammiye Taasire Shabakehaye Ejtemaiye Majazi dar Sakhtare Khanevade', *Fasnameye Farhangi-Tarbiyatiye Zanan va Khanevade*, **11**(35): 151–170.
- Farwell, J. P. and D. Arakelian (2013), 'What does Iran's Cyber Capability Mean for Future Conflict?' *Journal of Diplomacy and International Relations*, **14**(1): 49–58.
- Farwell, J. P. and R. Rohozinski (2011), 'Stuxnet and the Future of Cyber War', *Survival*, **53**(1): 23–40.
- Golkar, S. (2011), 'Liberation or Suppression Technologies? The Internet, the Green Movement and the Regime in Iran', *International Journal of Emerging Technologies and Society*, **9**(1): 50–70.
- Golkar, S. (2012), 'Cultural Engineering under Authoritarian Regimes: Islamization of Universities in Post-Revolutionary Iran', *Digest of Middle East Studies*, **21**(1): 1–23.
- Guerriero, C. (2019), 'The Political Economy of (De)Regulation: Theory and Evidence from the US Electricity Industry', *Journal of Institutional Economics*. <https://doi.org/10.1017/S1744137419000535>
- Guitton, C. and E. Korzak (2013), 'The Sophistication Criterion for Attribution: Identifying the Perpetrators of Cyber-Attacks', *The RUSI Journal*, **158**(4): 62–68.
- Guriey, S., N. Melnikov and E. Zhuravskaya (2019), '3G Internet and Confidence in Government', Discussion Papers 2019-13. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3456747 (accessed 10 February 2020).
- Habibzadeh, A. and R. Bakhshi (2016), 'Shabakehaye Ejtemaiye Majazi va Amniyyate Omumi', *Fasnameye Pajhouheshhaye Daneshe Entezami*, **18**(1): 1–34.
- Hamidi, Y., Y. Hamidi and S. Mehrbabak (2011), 'Localization versus Globalization of Social Networks', *Procedia Computer Science*, **3**: 191–196.
- Harper, D. A. and A. M. Endres (2018), 'From Quaker Oats to Virgin Brides: Brand Capital as a Complex Adaptive System', *Journal of Institutional Economics*, **14**(6): 1071–1096.
- Hosseinpour, J. and A. Momeni (2017), 'Taasire Shabakehaye Ejtemaiye Majazi bar Hoviyate Nahade Khanevade', *Fasnameye Barnameriziye Refah va Tovseye Ejtemai*, **8**(32):33–60.
- Ismail, A., T. Schött, A. Bazargan, B. Salaytah., H Al Kubaisi., M Hassen., I de la Vega., N Chabrak., A Annan and M Herrington. (2018), 'The MENA Region National Entrepreneurial Framework Conditions', in N. Faghih and M. R. Zali (eds), *Entrepreneurship Education and Research in the Middle East and North Africa (MENA)*, Cham: Springer, pp. 73–102.
- Jha, C. and O. Kodila-Tedika (2019), 'Does Social Media Promote Democracy? Some Empirical Evidence', *Journal of Policy Modeling*, <https://doi.org/10.1016/j.jpolmod.2019.05.010>
- Kanani, M. and M. Goodarzi (2017), 'Fostering New Technology-Based Firms in Iran: Inspiration of World Models in Solving Domestic Challenges', in A. Soofi and M. Goodarzi, *The Development of Science and Technology in Iran*, New York: Palgrave Macmillan, pp. 29–43.
- Karagiannopoulos, V. (2012), 'The Role of the Internet in Political Struggles: Some Conclusions from Iran and Egypt', *New Political Science*, **34**(2): 151–171.
- Karamelikli, H. and N. Alizadeh (2017), 'Iran İslami Bankacılık Sistemi Üzerine Bir Değerlendirme', *Bankacılık ve Sigortacılık Araştırmaları Dergisi*, **2**(11): 36–58.
- Kazanin, V. E. (2017), 'Telegram-Channels and Twitch-Broadcast as the Prospective Technologies in Government Transparency', *Contemporary Problems of Social Work*, **4**(12): 61–68.
- Kelly, J. and B. Etling (2008), 'Mapping Iran's Online Public: Politics and Culture in the Persian Blogosphere', *Berkman Center for Internet and Society and Internet and Democracy Project, Harvard Law School*.
- Kenney, M. (2015), 'Cyber-Terrorism in a Post-Stuxnet World', *Orbis*, **59**(1): 111–128.
- Khiabany, G. (2018), 'Citizenship and Cyber Politics in Iran', in M. Zayani (ed.), *Digital Middle East: State and Society in the Information Age*, New York: Oxford University Press, pp. 217–238.
- Kian, M. and Z. Qolipour (2016), 'Asare Tarbiyatiye Shabakehaye Ejtemaiye Telfone Hamrah bar Hoviyate Melli va Dini Daneshjuyan', *Resaneh*, **27**(2): 105–122.
- Kodila-Tedika, O. (2018), 'Natural Resource Governance: Does Social Media Matter?', MPRA Paper 84809, University Library of Munich, Germany.
- Kohl, U. (2017), *The Net and the Nation State: Multidisciplinary Perspectives on Internet Governance*, Cambridge: Cambridge University Press.

- Kumar, A., R. Balakrishna, U.G. Nandish and L. Naveen (2012), 'A Social Networking (Orkut) on Local Area Network with Client Server Architecture', *International Journal of Advanced Research in Computer Science and Software Engineering*, 2(1): 1–6.
- Lalmohammadi, N. (2016), 'Sarava Pars Venture Capital Firm: the Case of the Emerging Start-up Market of Iran', MA Thesis, Politecnico DI Milano, School of Industrial and Information Engineering.
- Lindsay, J. R. (2013), 'Stuxnet and the Limits of Cyber Warfare', *Security Studies*, 22(3): 365–404.
- Lourenço, A. and S. Turner (2019), 'The Role of Regulation In Constituting Markets: A Co-Evolutionary Perspective on the UK Television Production Sector', *Journal of Institutional Economics*, 15(4): 615–630.
- Lu, J. and X. Liu (2018), 'The Nation State in the Digital Age: A Contextual Analysis in 33 Countries', *International Journal of Communication*, 12: 110–130.
- Marczak, B., J. Dalek, S. McKune, A. Senft, J. Scott-Railton and R. Deibert (2018), 'Bad Traffic: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?' The Citizen Lab, <https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/> (accessed 21 October 2019).
- Mazzucato, M. (2011), *The Entrepreneurial State*, London: Demos.
- Memar, S., S. Adlipour and F. Khaksar (2012), Shabakehaye Ejtemaiye Majazi va Bohrane Hoviyat, *Faslnameye Motaleat va Tahqiqate Ejtemai dar Iran*, 1(4): 155–176.
- Mirfardi, A., M. Mokhtari and A. Valinejad (2017), 'Mizane Dindari va Ertebate an ba Estefade az Shabakehaye Ejtemaiye Interneti', *Jamee Shenasiye Karbordi*, 28(66): 1–16.
- Mohaddes, K. and M. H. Pesaran (2013), 'One Hundred Years of Oil Income and the Iranian Economy: A Curse or a Blessing?' in P. Alizadeh and H. Hakimian (eds.), *Iran and the Global Economy: Petro Populism, Islam and Economic Sanctions*, New York: Routledge, pp. 28–61.
- Mohammadi, A., A. H. Yavari and M. Javanmard (2017), 'Naqshe Shabakehaye Ejtemaiye Majazi dar Ijade Bohranhaye Ejtemai', *Faslnameye Pajhouheshhaye Daneshe Entezami*, 19(1): 1–24.
- Moshiri, S., M. M. Parsa and L. Darugar (2018), 'Barrasiye Asare Fannavariye Ettelaat va Ertebatat bar Zancireye Tovliide Kala va Khadamate Iran ba Estefadeh az Jadvale Dadeh-Setande', *Faslnameye Pajhouheshhaye Eqtesadi*, 18(68): 1–44.
- Naghbilasadat, S. R., F. Qasabi and P. Farhadi (2015), 'Iranian and Non-Iranian Social Networks' Structures; A Comparative Study', *Online Journal of Communication and Media Technologies*, 5(3): 91–106.
- Nasab, E. H. and M. Aghaei (2009), 'The Effect of ICT on Economic Growth: Further Evidence', *International Bulletin of Business Administration*, 5(2), 46–56.
- Ostrom, E. (1990), *Governing the Commons: The Evolution of Institutions for Collective Action*, New York: Cambridge University Press.
- Pieterse, J. N. (2012), 'Leaking Superpower: WikiLeaks and the Contradictions of Democracy', *Third World Quarterly*, 33(10): 1909–1924.
- Polanyi, K. (1944 [2001]), *The Great Transformation*, Boston: Beacon Press.
- Qasemi, V., S. Adlipour and M. Kianpour (2013), 'Taamol dar Fazaye Majaziye Shabakehaye Ejtemaiye Interneti va Tasire an bar Hoviyate Diniye Javanan', *Din va Ertebatat*, 19(2): 5–36.
- Qin, B., Strömberg, D. and Wu, Y. (2017), 'Why Does China Allow Freer Social Media? Protests versus Surveillance and Propaganda', *Journal of Economic Perspectives, American Economic Association*, 31(1): 117–140.
- Rahimi, B. (2011), 'The Agonistic Social Media: Cyberspace in the Formation of Dissent and Consolidation of State Power in Postelection Iran', *The Communication Review*, 14(3): 158–178.
- Rahimi, B. (2015), 'Censorship and the Islamic Republic: Two Modes of Regulatory Measures for Media in Iran', *The Middle East Journal*, 69(3): 358–378.
- Razavi, S. A. M., N. Nematifar and S. H. Muosavi (2018), 'Barrasiye Rabeteye Savade Resanei va Tahajome Farhangi dar Shabakehaye Ejtemai', *Eslam va Motaleate Ejtemai*, 6(2): 152–178
- Reinsberg, B. (2019), 'Blockchain Technology and the Governance of Foreign Aid', *Journal of Institutional Economics*, 15(3): 413–429.
- Rid, T. and B. Buchanan (2015), 'Attributing Cyberattacks', *Journal of Strategic Studies*, 38(1–2): 4–37.
- Rostami, M., R. J. Oskoi, E. Neshat and M. R. Forqani (2017), 'Barrasiye Tasire Shabakehaye Ejtemai bar Farhang va Bavarihaye Dini (Hoviyat) Karbaran', *Olume Ejtemaiye Danshgahe Azade Eslami Shushtar*, 11(2): 45–72.
- Safshekan, R. (2017), 'Iran and the Global Politics of Internet Governance', *Journal of Cyber Policy*, 2(2): 266–284.
- Salamzadeh, A. and K. H. Kesim (2017), 'The Enterprising Communities and Startup Ecosystem in Iran', *Journal of Enterprising Communities: People and Places in the Global Economy*, 11(4): 456–479.
- Salavatian, S. and M. Dovlatkhan (2017), 'Taasire Estefade az Shabakehaye Ejtemaiye Mobayli bar Hoviyate Farhangiyeh Daneshjuyan', *Rasaneh va Farhang*, 7(1): 49–66.
- Saleh, N. (2012), 'Egypt's Digital Activism and the Dictator's Dilemma: An Evaluation', *Telecommunications Policy*, 36(6): 476–483.
- Sammaknejad, B. (2017), 'The Impact of the Joint Comprehensive Plan of Action on the Startup Ecosystem in Iran', MA Thesis, SRH University of Applied Sciences Berlin, Germany.

- Seyyedalitabar, S. H., M. Pouravari, M. H. Asgarovladi and Z. Mohammadalipour (2015), 'Moqayeseye Negaresh be Ravabete Fara-zanashuyi va Jahatgiriye Mazhabiye Karbaran va Gheyrekarbarane Shabakeye Ejtemaiye Facebook', *Khanevadeh Pajhohi*, **11**(43): 297–308.
- Sharafaddin, H. and M. J. N. Eqbali (2016), 'Avamele Sakhtariye Bitaqvayi dar Shabakehaye Ejtemai Sayberi', *Din va Ertebatat*, **23**(1): 109–136.
- Sharifi, M. and A. Shahrestani (2017), 'Barrasiye Rabeteye beyne Mizane Estefade az Shabakehaye Ejtemaiye Majaziye Mobayli (Telegram) ba Raftar va Akhlaqe Ejtemaiye Karbarane ba Ruykarde Dini', *Farhang dar Danshgahe Eslami*, **7**(3): 277–298.
- Sunstein, C. R. (2017), *Republic: Divided Democracy in the Age of Digital Media*, Princeton: Princeton University Press.
- Turow, J. (2011), *The Daily You: How the New Advertising Industry is Defining Your Identity and Your Worth*, New Haven: Yale University Press.
- Ziaieparvar, H. (2009), 'Jange Narme Sayberi dar Fazaye Shabakehaye Ejtemai', *Resaneh*, **20**(2): 9–49.
- Zuboff, S. (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York: Public Affairs.