# INTERNET FREEDOM:

*Snapshots of the Case of Iran*

TRANSPARENCY
FOR IRAN

**Authors:**

Resa Mohabbat-Kar
mohabbat-kar@transparency-for-iran.org

Nicolas Hausdorf
hausdorf@transparency-for-iran.org

# 1 part

chapter

# 2 part

chapter

# 1

## Overview

The ubiquity of new information and communication technologies influences and changes politics and societies worldwide, and their enthusiastic adoption by Iran's citizenry, heralding the outlook for sociopolitical change, has triggered drastic and pervasive counter-reactions by Iran's ruling establishment in the form of jammed satellite signals, censored websites, blocked Internet services and surveillance of communications, just to name a few. Already, this battle is increasingly focused on the Internet and Internet-based services, with Iran being considered as the "least free" country in terms of Internet freedom.[001] Meanwhile, a multiplicity of actors has aligned in order to counter the Iranian state's Internet censorship and information control. They range from governments, commercial and non-profit entities, to scholars and journalists. Significant monetary and non-monetary resources are being leveraged to meet the needs of Iran's netizens in the face of the state's stifling Internet policies, which, in return, allocates even greater resources to crackdown on connectivity and users alike. Consequently, the struggle for Internet freedom is in great part characterized by cycles of measures and countermeasures between advocates and opponents. As this dynamic suggests, the continuation of this cycle engenders a learning curve, which in return allows both sides to readjust individual measures as well as to formulate policies and strategies that could guide broader shifts. In this respect, Iran's stated aim to move towards a self sustained National Information Network, parallel to the global Internet, can be read as an example of such a strategic readjustment, responding to the complexities and costs encountered while trying to control cross-border information flows. Along the same lines, authoritarian learning has led to Iran's adoption of bandwidth throttling as a preferred and more subtle means of censorship and information control, thereby seeking to alleviate the fallout associated with a full-blown and clearly perceptible disconnection from the Internet.

On the other side of the equation, external measures address a bandwidth of issues and needs that are relevant to Iranian users, ranging from the development and distribution of tools to circumvent censorship, training of activists, bloggers, and journalists on the safe use of these tools as well as digital security in general, rapid response to quickly emerging digital threats, and digital initiatives that provide otherwise suppressed and censored information, just to name a few. In addition to these programs, commercial and other private entities add to the equation, for example in the form of broadcasters utilizing circumvention tools to distribute their content to audiences inside Iran, or web hosting companies disabling Iranians' accounts with reference to US government sanctions.

As much as the diversity of the coalition of Internet freedom advocates constitutes a clear strength that has allowed an offer of relief in response to the Iranian government's isolationist Internet policies, so does it add layers of complexity when thinking about coordination and efficiency. The multiplicity of actors and actions, the complexity of identifying causalities between the range of external measures and their impact on the situation inside Iran, as well as nuances in stakeholders' strategies and priorities make it difficult to capitalize on accumulated learning experiences to the end of efficiency of Internet freedom efforts.

## Methodology and Objectives

This report results from our attempt to probe into the learning experiences of those stakeholders who, in their respective capacities, are part of the above mentioned reaction cycle, and whose actions and policies aim to advance the free flow of information and the security of Ira-

click ☞ [001] / *Freedom House (2013)-"Freedom on the Net"* nian's communications. The overall goal of this report is to contribute to a refinement of measures and policies that work towards that end.

In order to navigate these interconnected measures that impact on Iran's online environment, and to be able to identify instances where an adjustment of measures and policies could improve results, we turned to various individuals working at the intersection of digital freedom of expression and digital security. In a wide range of extensive interviews, we consulted experts from both the Iran focused community as well as from the wider Internet freedom community, technologists, practitioners, and researchers with year-long experience in the field. A subsequent careful evaluation of interviews, numerous follow-up discussions, accompanied by a review of additional research contributions, resulted in an overview of relevant developments in Iran's online environment and, most importantly, of strengths and shortcomings of a range of outside efforts currently addressing Iranian users. Subsequently, during August 2013, we received 18 of those experts interviewed before - ranging from diaspora civil society organizations, the technical community, digital security trainers, funders and researchers, all contributing to Internet freedom related goals, most of whom focus directly on Iran -  for a 3 day focus group discussion in Berlin in order to elaborate on and substantiate initial findings. What we have obtained during this time is a rich trove of opinions and analyses which provide insights into the experience of the multiplicity of our discussion partners who have been observing and *reacting* to Iranian Internet policy developments for a number of years, and therefore, by virtue of their experience, have drawn critical lessons which could help to refine measures and policies that seek to resonate with Iran's online environment and Internet users.

In this report, we draw on these insights in order to formulate suggestions that could raise the impact of certain Internet freedom measures. It is not within the capacity of this report to provide an exhaustive assessment of the entire range of activities that are addressed through Internet freedom programs, nor does it assert to embrace the entire breadth of variables that feed into the overall problematic of connectivity and security of Iranian Internet users.

Rather, our focus has been guided by topics that were of heightened concern to the consulted actors and that seemed to evoke pressing need for elaboration and discussion, which pointed us towards potentials and limitations that our discussion partners had identified and encountered while interacting with Iranian users, developing or carrying out initiatives that address audiences inside Iran. *By presenting a curated collection of these perspectives and learning experiences, we amplify the recurring themes and topics, while leaving us the opportunity to add our own analyses, in order to tease out suggestions on Internet freedom measures and policies that can help to address those potentials and limitations.*

## *Structure*

*Before* turning to this discussion, Part 1 of this report investigates the status quo inside Iran by describing the Iranian government's governance of the Internet (Pt 1, Ch.1), the range of obstacles with which the state sabotages Iranian's connectivity and compromises digital security (Pt.1, Ch.2), as well as by providing snapshots of user-dynamics (Pt.1, Ch.3). By outlining relevant *internal* developments that characterize Iran's repressive online environment, we provide layers of context which can assist the reader in putting into perspective Part 2 of this report- although both parts could also be read independently. In Part 2 we process our discussions on a range of *external* efforts that aim to respond to these developments. *To this end, we move along five distinct thematic categories that mirror and bear witness to the above mentioned recurring narratives and focal points that emerged from our stakeholder consultations.*

« content

Part 2, Chapter 1 presents a brief conceptual discussion on "established", i.e. dominant Internet freedom policies, and indicates their implications and limitations in the case of Iran. In reference to the issue of "outreach to Iranians", Part 2, Chapter 2 provides an example of an approach that seeks to alleviate the limitations indicated in the previous chapter as far as possible. In this chapter we also call attention to structural shortcomings prevalent to the community of outside actors represented by our discussion partners, which hamper the efficiency of their work. Part 2, Chapter 3 summarizes our discussions on the development and implementation of digital security education. In Part 2, Chapter 4, we attempt to outline patterns and dynamics of circumvention tool usage, and to derive implications that could guide investments in this field. In Part 2, Chapter 5 we highlight the detrimental effect of US government sanctions on Iranian's Internet experience. Lastly, with Part 2, Chapter 6, we include in this report an external contribution provided by one of the consulted experts, which explores the looming National Information Network in search of opportunities and dynamics that could counteract the agenda that the Iranian government is trying to advance with this project.

During the course of our research, we were confronted with what seems to be a common thread that - beyond the specific case of Iran - underlies a lot of the debates within the broader Internet freedom community, and which also reflects the strategic dimension involved in the struggle for advancing online capacities in repressive environments: the challenge of finding the right balance between initiatives that focus on assisting the activities of smaller audiences of important multipliers and committed activists, and investments in programs that also encompass other, broader audiences.[002] Unsurprisingly, this challenge also resurfaced during our consultations with several experts and on varying topics. In the case of Iran, there appears to be at least a marginalization of the latter approach. This observation found its expression in repeated calls for initiatives that would not by design limit the size and type of audience that could be reached inside Iran, due to their confrontational, contentious nature, for example.  This reasoning takes great account of the sociopolitical context on the ground, and the limitations it bestows on too narrow approaches. On the other hand, it can be read as a call to explore possibilities where, under the current circumstances, Internet freedom programs could contribute to more open online environments. In this report, we try to make these calls more explicit. In the discussions and suggestions presented here we err on the side of user-inclusion and avoidance of confrontation where possible, in order to expand the reach of Internet freedom programs to broader audiences.

[002] / The question of size, type of audience, and activities that should be assisted appears to transcend discussions on different topics. This is mirrored in deliberations on which type of audience circumvention tool developers should best focus on, see *Berkman Center for Internet & Society (2011) - "The Evolving Landscape of Internet Control*" or what type of content and online activities should best be promoted by Internet freedom programs. See *Zuckerman, Ethan (2010) - "Internet Freedom: Beyond Circumvention*"

## *Legal, Institutional*

Restrictions of the Iranian Internet can be legally traced back to the 1986 Press Law, a wartime piece of legislation ensuring the "propagation of Islamic culture and sound ethical principles". The law provides similarly ambiguous and interpretable suggestions like its pretensions of securing against "insulting Islam", "damaging the foundations of the revolution", "spreading rumors" or "propaganda against the state," for which it provides harsh punishments from long term prison sentences up to the death penalty. This Press Law had been amended both in 2000 and 2009 to include online publications. On June 28, 2009, amidst the nation-wide protests sparked through the June 12 presidential elections, a second legal pillar was introduced in order to close the loopholes of the existing legal mechanisms of Internet controls. The Computer Crimes Law (CCL) finally formalizes surveillance and filtering of online contents, by granting law enforcement authorities an upgraded mandate to regulate electronic and Internet based expression. The creation and consumption of banned online content has been effectively criminalized by the CCL, with sanctions including the death penalty, lengthy custodial sentences, draconian fines, and orders to close organizations, revoke licenses and ban individuals from using electronic communications.[003] Here again, essential elements of offenses are worded ambiguously, so that a wide range of legitimate expression and online behavior is potentially criminalized (publishing materials against "public morality and chastity"). The CCL further makes ISPs and other service providers like blogging platforms criminally liable for "forbidden" content displayed on their servers, thereby incentivizing the private sector to facilitate the government's Internet control mechanisms. ISPs are obliged to record all traffic data of their costumers for a period of six months.

These legal provisions are similarly the foundation for the institutional control apparatus which operates both on a political as well as regulatory level. The regulatory process is politically constrained, as the Communications Regulatory Authority, which grants licenses to the entire range of telecommunications entities such as ISPs and mobile operators, is subordinate to the Ministry of Information and Communication Technology (MICT). The regulatory process as well as the legal provisions described above effectively subject telcos operating inside Iran to the government's restrictive measures and policies. Politically, one of the key institutions is the Supreme Council on Cyberspace (SCC). Established in March 2012, this institution makes cyberspace policies a matter of the highest circuits of power in Iran, as it was established upon a directive of Supreme Leader Ayatollah Khamenei. The council itself consists of top ranking Iranian officials from a multitude of high level state functions[004], and is charged with formulating an overarching grand strategy for Iran's cyberspace policy, and overseeing and coordinating its bureaucratic and technical implementation.[005] The SCC has declared its directives as binding on all Iranian institutions operating in the field of ICTs. According to statements made by high ranking officials, the SCC's agenda includes the management of all activities and institutions charged with cyber defense capacities, the technical maintenance and development of the network infrastructure, as well as the formulation of guiding policies with respect to filtering and

[003] / *Article 19 (2012) – "Islamic Republic of Iran - Computer Crimes Law"*

[004] / They are the President, the Head of Judiciary, the Secretary of the Supreme Council, the Chairperson of the Majlis of the Cultural Committee, the Majlis Speaker, the Commander of Sepah, the Chief of National Police, the Minister of ICT, the Intelligence Minister, the Chairman of the Organization of Islamic Propaganda, the Minister of Science, Research and Technology, the Minister of Islamic Guidance, the Head of IRIB (national broadcaster) as well as seven Representatives of the Supreme Leader

[005] / *ASL 19 (2013) – "Sepah's Growing Media Activity"*

monitoring of web content and traffic.[006] One of the first and most complex tasks of the SCC will be the bureaucratic and technical implementation of the National Information Network.[007] Complementing the SCC's macro level approach, the Committee to Determine Instances of Criminal Content (CDICC) constitutes the second institutional cornerstone, responsible for the routine business of online censorship. Seven of its members simultaneously act as members of the SCC. The CDICC's task is to identify undesired content and report it to the Telecommunications Company of Iran, which, due to its oversight of the entire public Internet traffic, is responsible for the technical implementation of the filtering decision.

Nonetheless, despite the council's central and ultimately decisive standing, one can apperceive the continuing involvement of a multitude of institutions in the governance processes of the Iranian Internet, notably the Ministry of Information and Communications Technology, which oftentimes takes the role of communicating policy changes and developments of the Internet status quo, as well as bearing responsibility for the implementation of sanctions against websites violating online content regulations and the implementation of a National Internet Infrastructure.[008] Similarly, given the plethora of institutions involved in censorship - like the Information Communication Technology Section of Iran's Police Forces or Iran's cyber police unit FATA - the day-to-day operations of filtering is conducted in an arbitrary manner, despite the fact that institutions like the CDICC were intended to formalize and rationalize the process of filtering and to create the impression of a transparent and lawful procedure. Quite to the contrary, websites are regularly filtered without notification of the owner, or, in other instances, websites are blocked and unblocked within a matter of days and without explanation, and the CDICC itself has been challenged by a conservative member of parliament to have overstepped its competencies in filtering websites instead of weblogs.[009]

## *Basic Architecture*

Generally, Iran is oscillating between characteristics that would make it apt to be described either as an *Internet desert* or an *Internet oasis*. According to the Internet measurement company Renesys, Iran's domestic network infrastructure and ISP ecosystem can be considered as one of the fastest growing and most sophisticated in the region. The development of a robust and fast domestic network is said to be a byproduct - or requirement, respectively - of Iran's effort to engineer a self-sufficient national Internet. As a metric for the depiction of Iran as an Internet oasis, one can refer to the number of Iranian autonomous systems[010] (AS), which has exponentially increased in recent years, by far surpassing the growth rate of other countries in the region.[011] By receiving the status of an autonomous system, an organization appears in the global routing table and can *potentially* choose its own path to the global Internet by directly connecting to other peers. In a similar vein, in 2012, the fiber-optic cable system Europe Persia Express Gateway (EPEG) was created, establishing a low-latency connection from Western Europe to the Middle East, cross-

[006] / *Iran Media Program/ASL 19 (2013) – "Supreme Council on Cyberspace"*

[007] / Will be explained below

[008] / *Small Media Foundation (2013) - "Iranian Internet Infrastructure and Policy Report (March)"*

[009] / *Ibid.*

[010] / ASs are registered organizations - like banks, ISPs, companies, universities etc. - whose network connectivity is visible on the global Internet routing table. The interconnection of ASs‘ constitutes the Internet.

[011] / *Renesys (2013) - "Three ways Iran's Internet can show heroic flexibility"*

ing Iran from north to south.[012] As it is pointed out, “(...) Iran is sitting astride one of the most important Internet traffic corridors in the world, just by virtue of its geographic position and its EPEG consortium membership”.[013] Iran is therefore said to feature the basic conditions of a regional Internet hub, which in turn could serve as a prerequisite for the development of a diverse Internet ecosystem and economy. Regardless of these *potentials*, the predominantly security-driven management of the sector has prevented such a scenario.

In 2001, Supreme Leader Ali Khamenei consolidated control over the Internet through a decree that centralized provider’s connections to the international Internet.[014] Thereby, all private and semi-private ISPs are obliged to buy their bandwidth from a state controlled provider – the Telecommunications Company of Iran (TCI), which provides fixed and mobile infrastructure throughout the country. It is this reliance on one bottleneck and point-of-failure for international traffic that paves the way for deliberate state sponsored control mechanisms (see Part 1, Chapter 2) as well as considerable network instability and vulnerabilities of international traffic.  Iran’s international connectivity has consequently been measured as one of the most unstable in the world.[015] Furthermore, the monopolization of access and the absence of market-competition results in the regime charging one of the highest prices for end user Internet access in the region.[016]  Therefore, any liberalization attempts of the present ICT market would not only have to deal with the political security concerns, but also with the economic interest of security organizations like Iran’s Revolutionary Guards Corps, who have come to  generate considerable hard currency revenue by controlling the main provider of connectivity, the TCI.

The state of the mobile phone market bears resemblance to that of ISPs, as the incumbent providers Mobile Communications Company of Iran (owned by TCI), MTN-Irancell and Rightell are all owned by state or state-affiliated institutions.[017] Nevertheless, the mobile telephone market continues to grow at a penetration rate of 76.9%[018], with forecasts displaying considerable growth potential for cellular subscriptions and mobile data services[019]. Mobile operator Rightel has been providing and expanding 3G coverage since 2012.

Iran’s fourth five-year development plan (2005- 2010) aimed at expanding the country’s fixed broadband infrastructure with 1,5 million high-speed Internet connections nationwide managing to supply high-speed fiber-optic cables to approximately 250,000 users, thereby doubling existing structures. However, in 2006 the Ministry of Communications and Information Technology reconsidered its policy and forbid ISPs in supplying Internet access faster than at 128 kilobytes per second, effectively sabotaging the establishment of a multimedia online culture. Exceptions to this law, however, are numerous, with doctors, a range of professionals, as well as university students being allowed to access the Internet using faster bandwidth as well

[012] / *Renesys (2013) - “Gulf States Turn to Iran, Russia for Internet”*

[013] / *Renesys (2013) - “Three ways Iran’s Internet can show heroic flexibility“*

[014] / *Open Net Initiative (2009) - “Country Chapter: Iran”*

[015] / *See for example Small Media Foundation (2013a) –“Iranian Internet Infrastructure and Policy Report – January”* or *Seclists.org (2012) –“BGP Update Report”*

[016] / *NCRI (2013) - “Iran: High prices for ‘jammed and censored’ Internet”*

[017] / *Freedom House (2012) - “Freedom on the Net 2012 -Country Profile: Iran”*

[018] / *ITU (2012) –“Mobile cellular subscriptions“*

[019] / *Euromonitor International (2013) – “Iran’s expanding mobile phone market”*

as providers supplying higher bandwidth.[020] According to ITU standards, which measures high-speed Internet connections at a minimum of 1,5Mbit/s, less than one percent of Iranians have access to such connectivity.[021] A great part of the country, meanwhile, still uses dial-up connections to access the Internet (84 % according to a 2009 study by the Iran statistics center).[022]

Meanwhile, the physical connections of the Iranian Internet to foreign countries have remained limited to a total of 4 import/ export fiber optic link connections. They are at the Turkish border (Tellcom Superonline), at the Azeri Border to Russia (Delta, Rostelecom), to the UAE crossing the Persian Gulf (PCCW, Flag, Reliance, TI Sparkle, Telia), via the Gulf of Oman to Oman (EPEG). More fiber connections are export only and supply traffic to Turkmenistan, Afghanistan and Iraqi Kurdistan. The connections pay tribute to Iran's critical geostrategic situation and aim at avoiding overreliance on a single geopolitical counterpart.[023]

## *The National Information Network (NIN)*

Iran's Fifth Five-Year Development Plan (2010-2015) outlines the development of a National Information Network for the purpose of "e-government services, industry, information technology, information literacy, and increased productivity in the areas of economic, social and cultural activities."[024] The crucial feature of the National Information Network is its intended autarky from the global Internet. Accordingly, a user request for content and services would not have to leave the national infrastructure on its way to the destination server. Efforts have been made to move relevant public and private institutions like government ministries and affiliated institutions, banks and universities to servers based inside Iran[025]. Official statements indicate that more than 90 percent of government websites have already been moved to domestic servers. A similar strategic readjustment by private businesses and websites has yet reportedly to follow suit on a meaningful scale.[026] Crucial to the government's strategy will be the development of localized and domestically hosted online services and applications capable of compensating for their popular foreign counterparts like Google search, Gmail, YouTube, Facebook, Twitter and similar services. The success of a suchlike endeavor meanwhile remains questionable: while announced services like the *Parsjioo* search engine[027] or Google Earth surrogate *Basir* are yet to be officially launched, existing ones like the national e-mail service[028] and video-sharing platform *Mehr.ir* have failed to attract a critical mass of users.[029] Suchlike attempts therefore cast doubt upon the reassurances of officials[030] to remain connected to the global Internet, yet also provide proof of the very practical challenges the regime is facing

[020] / *Iran Media Program (2012) - "Finding a Way- How Iranians reach for news and information"*

[021] / *Trend.az (2012)- "Less than one percent of Iranians have high-speed Internet access"*

[022] / *Open Net Initiative (2009) - "Country Chapter: Iran"*

[023] / See for example *Renesys (2013) - "Three ways Iran's Internet can show heroic flexibility"*:or *Open Net Initiative (2013) – "After The Green Movement"*

[024] / *Anderson, Collin (2012) – "The Hidden Internet of Iran"*

[025] / *Freedom House (2013) - "Freedom on the Net – Country Profile: Iran"*

[026] / Ibid.

[027] / *Trend.az (2012) – "Iran establishes own online search engine"*

[028] / *The Guardian (2013)- "Iran launches 'National Email Service"*

[029] / *Freedom House (2013) - "Freedom on the Net – Country Profile: Iran"*

[030] / *Trend.az (2012) – "Minister denies claims Iran plans to disconnect itself from the Internet"*

in a project which appears both costly and fraught with risk.

Generally, it is worth taking a closer regard at the objectives the Iranian regime is hoping to attain by enforcing the implementation of the NIN: As data stored or moving on the domestic infrastructure is within immediate reach of the authorities, content deemed inflammatory or undesirable will be deleted at ease or entirely prevented in the first place. The NIN at least potentially allows for a monitoring of the entire range of communications. Officials further claim the prevention of foreign spying and cyber-attacks as a benefit of a self-sustained network[031], as well as a generally improved connection in terms of speed and reliability.[032] The NIN thus appears as both a promise of increased security and political control as well as the supply of a modern IT communications infrastructure[033] inside Iran. The NIN has thus become an object of rumors and fears, and little knowledge about it can in light of the regime's information policy reliably be claimed. Regardless of political rhetoric and mediatized debates, changes in the domestic infrastructure and user experience provide circumstantial evidence. Researcher Collin Anderson has established the coordinated adoption of private IP addresses by Iranian ISPs and government agencies, outlining a network that is only reachable from within Iran.[034] According to a directive by the Communications Regulatory Authority, service providers inside Iran have prepared their servers to respond to two separate sets of Internet addresses, effectively allowing the operation of two different networks - one public, one private.[035] The extent to which domestic service providers and institutions have acquired private IPs is not known.[036] The prospect of not being reachable within the NIN during times of disconnection from the global Internet certainly serves as an incentive for providers to connect to the private network. Along the same lines, the increasing number of registered autonomous systems inside Iran (see above) has been interpreted as preparatory operations by providers and institutions in order to ensure their availability and interconnectedness on the NIN.[037]

In order to facilitate the transition of a meaningful number of Internet users to the domestic network, services and applications, one strategy for the government is to incentivize its use, or to disincentivize international connectivity and services respectively. According to Iran's new communications minister Mohammad Vaezi, the Ministry has added 15 GB to the nation's internal traffic, with further plans to increase domestic bandwidth, and to boost the overall number of Internet users by ensuring access in rural areas and villages.[038] Users already experience a considerably faster connection when accessing content hosted on the NIN infrastructure, as compared to the global Internet.[039] Another incentive, as suggested by officials, will be the reduced costs of Internet access, which currently can be observed to act as an impediment to a popularization of access. Domestic routing of traffic would reduce depen-

[031] / *Trend.az (2012) - "Minister: Iran's National Net to counter all cyber attacks"*

[032] / *Anderson, Collin (2012) – "The Hidden Internet of Iran"*

[033] / Behabadi has claimed that the loading of websites hosted inside Iran will be 10 times faster than outside. *See also Small Media (2013)*

[034] / *Anderson, Collin (2012) – "The Hidden Internet of Iran"*

[035] / *Freedom House (2013) - "Freedom on the Net – Country Profile: Iran"*

[036] / *Anderson, Collin (2012) – "The Hidden Internet of Iran"*

[037] / *Renesys (2013) - "Three ways Iran's Internet can show heroic flexibility"*

[038] / *Small Media Foundation (2013) - "Iranian Internet Infrastructure and Policy Report (July-August)"*

[039] / *Freedom House (2013) - "Freedom on the Net – Country Profile: Iran"*

dency on costly international traffic, which in turn could result in low-cost access to the NIN.[040] Given the severity of deliberate state sponsored interferences in *international* traffic, as well as the vulnerabilities that accompany the security-driven reliance on one bottle-neck to ensure the international connectivity of an entire population, the prospects of a fast, reliable, accessible and affordable domestic network clearly outlines the government's double-track strategy of "carrots and sticks". In fact, one may argue that the currently practiced disincentive of international connectivity suffices in terms of "natural selection". Whether or not the final shape of the NIN includes a permanent and de facto segregation from the global Internet meanwhile remain subject to speculation. The existence of a parallel domestic network accommodating vital administrative and financial traffic would certainly reduce the costs of a disconnection during times of heightened political tensions. It remains to be seen, to which extent Iranian users will accept and become regular users of  the NIN, and how the correlation of a fast and widely accessible, but nevertheless tightly monitored and sanctioned domestic network changes Iran's online dynamics.

[040] / *Small Media Foundation (2013) - "Iranian Internet Infrastructure and Policy Report (July-August)"*

## Strategies and Tactics

One way to grasp the complexity of Internet control in Iran is to conceptualize the online environment as being comprised of a *principally* unimpeded flow of information and communications, constrained by a variety of state sponsored disruptive interferences. According to the most common explanation, interferences are supposed to disrupt those flows of information and communications that contravene domestic political discourses or decompose the religious-moral, ergo cultural fabric of society. Especially the latter justification refers to and tries to curb a long term and insidious process of cognitive change towards "westernization" of Iranian "hearts and minds". This line of argumentation does not constitute a historic novelty, as it reaches back to the UNESCO debates of the 1970s and 80s surrounding the New World Information and Communication Order - it therefore precedes the era of the Internet, and was just given greater urgency with the advent of ubiquitous online communications.

Other aspects that feed into the overall reasoning behind Iran's disruptive interferences in online flows are not as popularly discussed as the above notion of "cultural osmosis" - albeit being critical to Iran's perception of the Internet. At a time when cyber warfare is of paramount importance to, and tops the agenda in ministries, public and private institutions, and think tanks across the globe, Iran is the agreed upon security concern at precisely the same institutions. In light of this conflict situation and experiences like Stuxnet[041], control over information flowing across domestic networks as well as international gateways becomes a national security priority and concern - and the National Information Network is its most extreme policy response. A range of external efforts that are aimed at using the Internet as a tool for political change and revolutionary agency  in Iran further add to Iranian authorities' perception of the realm as a foreign controlled and subversive attack tool. This facilitates an understanding of the Internet as a gateway for political instability, prompting disruptive interferences as an obvious policy response.

On a micro, or tactical level, the regime of disruptive interferences is highly responsive to external developments. Internet control is rather a dynamic process than a destination, constantly translating the ongoing changes in the social and political landscape and agenda into varying scopes and scales of interferences. Ever since websites operated by conservative bloggers or affiliated with high ranking officials like former President Rafsandjani and at that time acting President Ahmadinedjad[042] were being firewalled, the portrayal of the struggle over the Internet in Iran as merely a battle between a ruling establishment and processes of democratization becomes obsolete. Reflective of the outcome of domestic power struggles as well as relevant events and developments, websites and resources are blocked and unblocked, information flows throttled and normalized "just in time": amidst a free fall of the Iranian currency, websites keeping track of exchange rates have been filtered[043] in early 2013, and tools for circumventing blocked websites or Voice over IP applications that were accessible throughout 2012 were blocked in the immediate run-up to the presidential elections of 2013, just for being restored again shortly thereafter.[044]

Furthermore, there is the notion of a "cat-and-mouse game" between the censorship apparatus on the one hand, and users and circumvention tool developers on the other. In this respect, a timed and/or temporary disruption of on-

[041] / *New York Times (2012) - "Obama Order Sped Up Wave of Cyberattacks Against Iran"*

[042] / *Guardian (2012) - "Iran's censors wage web war against Ahmadinejad as elections loom"*

[043] / *Kaleme (in Farsi)*

[044] / *Small Media (2013) - "Iranian Internet Infrastructure And Policy Report (June-July)"*

line resources and circumvention tools can - beyond the obvious motivations noted above - serve as a feedback mechanism for the regime, allowing the authorities to fine-tune and calibrate the scope and scale of disruptive interferences.  As the authorities block popular circumvention tools, they force developers to respond with technical adjustments. By deploying a technical solution, developers might leave digital footprints, disclosing valuable diagnostic information as an unintended by-product[045], which in turn could be exploited by the authorities to render the tool useless "just in time". The same applies to users, quickly searching for and shifting to surrogate solutions, thereby bringing alternative tools to the attention of the censors and watchers. Along the same rationale, but from a non-technical perspective, disruptive interferences, particularly those targeting "indispensible" services like Google's search engine or e-mail service, can serve as a means to test popular sentiment, allowing the regime to approximate the public's acceptance limit. The stakeholders and institutions adhering to the pervasive control apparatus have to broker and compensate the associated costs of disruptions- even in Iran. The public outcry after the blockage of Google was just the most conspicuous articulation by the camp opposing the pervasive disruptions - a camp that reaches all the way into the political institutions, growing in size and diversity. The actual technical implementation of disruptions is inextricably linked with the problem of precision, aiming at the best case scenario of disrupting a designated flow while sparing others. The technical challenge thereof produces a high error-rate and widespread collateral damage.[046] In this context, the authorities' increasing reference to "smart filtering" [047] is indicative of their concern for the steadily rising economic, social and political costs of pervasive and blanket disruptive interferences.

## *Scope and Scale*

Legal, regulatory and institutional developments (Part 1, Chapter 1) have made possible the establishment of a physical network architecture that allows all sorts of disruptive interferences *by design*. State-mandated control mechanisms are implemented in a centralized as well as de-centralized manner. Since the entire public Internet traffic has to pass through a state owned bottleneck (Telecommunications Company of Iran), a first layer of control is implemented on a national level. The state has added a second decentralized layer of control by forcing private consumer ISPs to implement disruptive policies in their respective network. Public Internet traffic is routed through domestic traffic monitoring centers that relay and log user requests (e.g. for a website) before deciding whether to allow or block the request.

Beyond the strategic and tactical considerations mentioned above, the authorities' actual capabilities (i.e. available resources and technical expertise) play a crucial role when determining the scale and scope of disruptive inter-

[045] / *Torproject (2011) - „Iran blocks Tor; Tor releases same-day fix"*

[046] / On a daily basis, „uncritical" and inoffensive websites inexplicably get blocked, just to be restored within days, at times even several hours.

[047] / *Khabaronline (in Farsi)* The stated aim is to block single controversial entries or sections of a given website /platform, rather taking down the entire site: With domestically hosted websites, authorities have repeatedly ordered hosting companies to remove single posts. Foreign based platform  Tumbler was unblocked, however the section hosting the site's media files was still inaccessible. "Smart control" software was specifically mentioned in conjunction with discussions on the "useful" parts of social networking platforms, which "smart filtering" is supposed to keep accessible, while blocking the "harmful" aspects. This discussion entered the discourse just weeks after Iran's Supreme Leader Ali Khamenei had joined Facebook. See also *Rferl (2013) - "Iran Developing 'Smart Control' Software for Social-Networking Sites"* or *weblognews (in Farsi)*

ferences. To outside observers, the assessment of these capabilities remains a challenge, and our understanding thereof is in parts based on circumstantial evidence.[048] Newly acquired or the full extent of capabilities are demonstrated only once they are deployed. Based on testing, user accounts, and monitoring activities of NGOs, it is safe to say that the control apparatus' capabilities regarding the scale and scope of disruptive interferences includes blocking of IP addresses, entire domain names, specific URLs, keywords and strings of letters in a URL and search requests, specific ports or protocols, traffic signatures identifying undesired tools and services and the redirection of DNS requests (DNS interception). Multiple techniques are applied simultaneously to eliminate possibilities of missing/ under-blocking undesired traffic flows (e.g. IP + signature/ URL). Through these identifiers, the control apparatus has managed to permanently or intermittently block access to websites (e.g. HRW or Facebook), search results (e.g. displaying websites containing information on circumvention tools), online services ( email, P2P instant messaging and VoiP services like WhatsApp, Viber and Skype), specific subsite-URLs, specific content types (audio/ video like Mp3, MP4, AVI), VPN services and purpose-built circumvention tools (e.g. Hotspot Shield or TOR). Regarding content that is hosted on domestic servers or involving in-country staff within the immediate reach of the authorities, the evolving strategy seems to shift from a publicly more perceptible blocking of websites to orders requiring providers and hosts to delete or take down content.[049]

Taken together, the application of the above mentioned identifiers creates an extensive network of control that has so far been implemented on ISP as well as a national level, at times creating a patchwork of varying degrees of accessibility of specific content across the country. In fact, one could speak of a trend regarding the location where information flows are inspected and judged upon, moving from a national level closer to the end-user (ISP level) - in this context, public statements have even referred to the production of filtering software for home and company users as well as real name registration as a requirement for Internet access, the latter of which is supposed to customize control based on user category.[050] The blocking of content is based on the pre-identification and categorization of undesired websites. As the volume of content and websites grow, basic techniques like keyword-based URL filtering present the control apparatus with certain imperfections, as the URL might not always be determinative of the desirability or undesirability of the website's *content*, especially if the URL does not contain designated keywords that would trigger the blocking.[051] To counter under-/ over-blocking, the control apparatus might strive towards a more dynamic inspection of the packets transporting the entire content (payload) of the website, instead of solely relying on shallow properties like URLs. Deep Packet Inspection (DPI) capacities serve this purpose, and based on observations regarding the scope and scale of control, it could be derived that Iran has acquired and implemented

[048] / This is a problem that stems from the inadequacy of available methods for conducting technical research. In some cases e.g. it is difficult to locate the place in the Iranian network where a blockage is implemented, or whether it is at all a matter of deliberate blocking: See for example *The Verge (2013) - "World Wide (Redacted):inside Iran's private Internet"*

For instance, conflicting accounts from the ground on the blockage of a website or VoIP application would allow the observer to conclude that the blockage has not been implemented nationwide, but instead on certain ISPs.

[049] / See for example *weblognews (in Farsi )* and *Alireza Shirazi (2012)*

[050] / *Mehrnews (in Farsi)*

[051] / The opposite case also applies, e.g. when a URL contains designated keywords that trigger the blocking, despite the fact that the content of the website is inoffensive - as demonstrated by the blocking of http://www.no-porn.com/ .

basic DPI capacities. DPI allows for a thorough investigation of the content of requested websites and a wide spectrum of personal online communications, as well as the manipulation thereof through removing certain sites within an otherwise accessible domain, or through deleting or rewriting text parts.[052] References to "smart control" might indicate the future implementation of DPI capacities for a more granular and dynamic filtering of websites. Nevertheless, it remains subject to speculation just how intrusive Iran's actual DPI capacities are or to what ends the authorities have managed to implement these capacities. Beginning in January 2011, authorities managed to pointedly disrupt encrypted traffic belonging to circumvention tools like TOR, Hotspot Shield, Ultrasurf and Freegate, by detecting signatures that allow the filtering machine to classify the traffic pattern as belonging to an undesired circumvention tool.[053] In February 2012 all SSL encrypted connections leaving the national network were blocked, while domestic traffic using the same protocol was unaffected. The full spectrum of Iran's DPI capacities was demonstrated in the run-up to the 2013 presidential elections. As unencrypted traffic (like http) was "only" subject to the usual content filtering, encrypted, standard web traffic (like SSL) was severely throttled and disrupted intermittently. Unclassified and random traffic was throttled and dropped after a short period of time (60 to 120 second), or outright blocked.[054] Although the history of Internet control in Iran is riddled with access restrictions on web content and services, the severity of the latest blocking campaign results first and foremost from the state's capacity to render useless the tools designed to circumvent the prevalent access restrictions. To avoid blocking through DPI, sophisticated circumvention tools try to obscure their traffic in order to not be detected. Iran's capabilities *and* willingness to handle all international connections according to a predefined "whitelist" of approved traffic made most of the existing circumvention mechanisms obsolete: "This approach would allow the censor to preemptively block new, unrecognized circumvention techniques."[055] Iran's newly acquired DPI "panic button" seems to have replaced the Internet "kill switch". Furthermore, Iranian officials have confirmed the use of bandwidth-throttling as a deliberate control strategy. Independent research published prior to the confirmation documents the use of this rather subtle form of disruption as one of the preferred ,and most effective mechanisms, as it can potentially affects every Iranian computer connected to the Internet.[056] The pace at which Iran's disruptive capabilities have gained sophistication prompts questions regarding the origin thereof. A great deal of reporting and research points to the acquisition of foreign technologies as the basis of Iran's advancements.[057] On the other hand, as a side-effect of decades of international sanctions, Iran has invested heavily in strengthening domestic capabilities in the production of hard- and software, as well as development of manpower at research institutes and institutions of higher education.[058] Government incubated high-tech greenhouses like the Pardis

052 / *Global Voices Advocacy (2009) - "Deep Packet Inspection and Internet Censorship: International Convergence on and "Integrated Technology of Control"*

053 / *Torproject (2011) - "New Blocking activity from Iran"*

054 / For a detailed account of the multi-stage blocking campaign during election season see *Small Media (2013) - "Iranian Internet Infrastructure And Policy Report (April-June)*

055 / *Aryan, Aryan, Halderman (2013) - "Internet Censorship in Iran: A First Look"*

056 / *Anderson (2013) - "Dimming the Internet- Detecting Throttling as a Mechanism of Censorship in Iran"*

057 / See for example *Bloomberg (2011)- "The Surveillance Market and Its Victims"* ; *Reuters (2012) - "Special Report: Chinese firm helps Iran spy on citizens"*, and *Citizenlab (2013)- "Some Devices Wander by Mistake"*

058 / Gabi Siboni and Sami Kronenfeld (2012) - „Iran and Cyberspace Warfare", in Military and Strategic Affairs | Volume 4 | No. 3 | December 2012

Technology Park and Guilan Science and Technology Park accommodate companies like AmnAfzar Ltd., which has developed a phalanx of hard- and software that can be used to control network traffic.[059] It is noteworthy that Amn Afzar Ltd., as well as its founder Rasool Jalili, have been targeted by the U.S. sanctions regime.[060]

While the blocking of tools and content tend to effect perceptible results, the ramifications of Iran's technology arsenal regarding surveillance are comparatively harder to assess. Generic information on the range of capabilities acquired through foreign commercial technologies does exist.[061] Accordingly, the authorities can geo-locate mobile phones and monitor the content of conversations and text messages.[062] Furthermore, given the existence of DPI capacities and traffic monitoring centers on the Iranian network, all non-encrypted *Web-based* communications can potentially be monitored and, due to legal requirements imposed on consumer ISPs, [063] be traced back to the individual user, which has happened on several instances. [064] Little is known about the technical details surrounding those communications events that lead to the arrest of users.[065] Despite the lack of legal layers of protection, the tracing of web-based communications to its point of origin does not come without administrative efforts.[066] Beyond perceptible blocking of web-content, tools, and applications, it is not known to what extent traffic monitoring centers and DPI capacities are effectively and purposefully utilized for the identification of users *on a mass scale*. The political economy of surveillance in present day Iran suggests other approaches to surveillance, that by no means have to be less effective. It is reasonable to believe that a more targeted surveillance of *persons of interest* serves as a starting point to map out social profiles of targets and the networks they are embedded in. The trend of self-broadcasting, i.e. the publication of personal information, views and affiliations in social media environments, facilitates the identification of key broadcaster and re-broadcaster and allows a mapping of relationships and dissent of transnational scale, effectively tapping into diasporic counterparts of domestic networks. From a cost-benefit perspective, one could argue that this rather targeted intelligence gathering is at this point in time more economical relative to efficiency for Iran when compared to the resources necessary to maintain a system of mass blanket surveillance because it allows for a sufficient output of intelligence at fairly low costs. The infiltration of discussion groups and

[059] / Ibid.

[060] / Separ and Parsgate are among the tools developed by AmnAfzar Ltd., allowing for „content filtering, traffic authentication, instant messaging (IM) and Peer - to - Peer (P2P) filtering, Voice over Internet Protocol (VoIP) monitoring and filtering": *US Treasury Department Office of Public Affairs (2012) - " Fact Sheet: Sanctions On Iranian Government And Affiliates"*

[061] / See *Bloomberg (2011) - "The Surveillance Market and Its Victims"* and *Citizenlab (2013) - "Some Devices Wander by Mistake"* and *Daily Mail (2012) - "Chinese sell Iran £100m surveillance system capable of spying on dissidents' phone calls and Internet"*

[062] / See for example *Bloomberg (2011) - "Iranian Police Seizing Dissidents get Aid Of Western Companies"* Furthermore, text messages have been blocked on multiple occasions due to banned keywords. The list of undesired keywords is continuously adjusted according to external social, political and economic events and developments.

[063] / ISPs are required to keep all data sent or received by their clients: *Press TV (2013) -"Iran to monitor cyberspace to fight offenses"*

[064] / According to victims and human rights groups, authorities have intercepted e-mails and IM of journalists and activists and presented transcripts thereof during interrogations. See *Bloomberg (2011)*.

[065] / It is not well researched and documented how exactly authorities gained access to private communications - whether through network surveillance, through malware and phishing or through interrogation of others. Similarly, it is not well documented in how far victims have practiced due diligence regarding digital communications security.

[066] / *The Atlantic (2009) - "Internet Surveillance and Iran: A Primer"*

online platforms[067] for the purpose of monitoring persons of interest and mapping opposition communities and networks points to the tip of the iceberg. A shifting trend from a mere reactive blocking of content and tools, to a more pro-active engagement in cyberspace seems to be indicative of the "satisfactory results" of this approach. The state sponsored compromise of certificates for secure encrypted online communications[068] in 2011, as well as the vast phishing campaign aimed at Iranian Gmail users[069] ahead of the 2013 presidential elections, were only the most publicized instances outlining a double-track strategy, where a sharp rise of "offensive" interventions, in the form of phishing, malware, and hacking, complements the "defensive" doctrine of blocking. Beyond fueling an online-climate of fear and insecurity, intelligence collection is certainly the central concern. Besides the above mentioned instances of phishing that were supposed to circulate at random among Iranian Internet users, the vast amount of attacks are seemingly meant to grant access to milieus where the attackers have spotted or assume dissenting voices. Domestic *as well as* foreign based journalists and civil society activists working on Iran related issues have increasingly been pointedly attacked with the aim to obtain login data to accounts and online platforms, either by redirecting victims to fake login pages, or by inserting malware customized to gain the victim's attention.[070] The successful compromise of accounts and communications of networked individuals in media and activism generates considerable intelligence output, as it potentially discloses a vast network of interconnected actors. Additionally, in several instances, the distribution of infected circumvention tools that are particularly popular among Iranian users serves not only to compromise communications and to map censorship evaders, but creates further collateral damage by creating a crisis of confidence regarding tools and paths of distribution.[071] It has been noted that the vast amount of these attacks are not characterized by technical sophistication[072], by implication relying on the addressee's inattention, or lack of due diligence. Beyond intelligence gathering, countless hacking and DDoS-attacks have severely and repeatedly disrupted the accessibility and operations of websites considered as hostile by Iranian authorities.[073] According to what has been described as "just in time" interference, these attacks intensify in times of heightened political contestation, which has been the case on several occasions in the run-up to the 2013 Iranian presidential elections. As yet another manifestation of a pro-active engagement in online spheres, we have seen disinformation and propaganda campaigns in an effort to counter the popularity of foreign based Persian language news media like Voice of America (VOA), Radio Farda and BBC Persian. Fabricated news and false allegations have been spread on duplicated Facebook accounts which claim to belong to staffers and journalists, fake blogs and even

[067] *Rferl (2013)- "In Iran, Beware of New Facebook 'Friends'"*

[068] *CNet (2011) - "Comodohacker returns in DigiNotar incident"*

[069] *Arstechnica (2013)- "Phishing attacks on Iranian Gmail users jump before Iranian election"*

[070] For a detailed description of the methods used see: *Small Media (2013) - "Iranian Internet Infrastructure And Policy Report (April-June 2013)"* and *"Iranian Internet Infrastructure And Policy Report (February-March2013)"*

[071] Malicious copies of circumvention tools like Simurgh and Psiphon have been distributed on popular file sharing sites: see for example *Citizenlab (2012) -"Iranian anti-censorship software 'Simurgh' circulated with malicious backdoor"* and *Psiphon Alert (2013)*

[072] *Small Media (2013) - "Iranian Internet Infrastructure And Policy Report (April-June)"*

[073] These attacks have targeted a diverse set of organizations, such as foreign hosted social media platform Balatarin, Persian language broadcasters and media organizations like Voice of America, Radio Farda, Radio Zamaneh, BBC Persia, and other Iran oriented sites. See for example *Small Media (2013)*

entire counterfeit news websites imitating VOA’s and BBC Persia’s web presence.[074] Against this background, it can be concluded that, over the past years, a network of hacker organizations and pro-regime online activist-communities has evolved, dedicated to advance the authorities’ offensive engagement in cyberspace , and thereby complementing the rather “passive” strategy of filtering. Some of these organizations and communities are officially under the control of the IRGC[075], others loosely affiliated or certainly welcomed by the authorities.[076]

[074] / *The Guardian (2013) - “Iran creates fake blogs in smear campaign against journalists in exile”*

[075] / The IRGC announced its command over the „Iran Cyber Army“, see *Radio Zamaneh (2010) - “Iran’s Revolutionary Guards claim “Iranian Cyber Army”*

[076] / *Rferl(2013) - ”Iran says it welcomes hackers who work for Islamic Republic”* Furthermore, Iran-based Ashiyane Digital Security Team has been described as one of the world’s most active hacking-collectives.

## *The Elusive User*

The image of Iran's Internet user is a rather elusive one. Not only is research on the subject heavily constrained by the repressive environment inside Iran, but also the available fragments of information are at times contradictory. Insights into the landscape of Iran's Internet users, their usage, and consumption patterns, has to be compiled through a series of studies conducted by select non-state[077]-, private sector, intergovernmental-, as well as Iranian state government-actors.

A first difficulty is encountered in judging the extent and relevancy of Internet use. The reliability of official data is questionable, as statements diverge widely. According to the new minister of ICT Mahmood Vaezi, in Iran there are 30 million Internet users along with 4,1 million high-speed Internet ports at a 41% Internet penetration rate[078], whereas, shortly before, the National Internet Development Center (NIDC) had announced that 46 million users were online in Iran along with a penetration rate of 61,57%.[079] The number of Internet users, however, does not indicate the pattern or the quality of use of the medium. In an extensive 2011 study[080] nearly half (47%) of users indicated themselves to be current users, a status assigned to anyone using the Internet more than once per week. It is meanwhile safe to assume that Internet access will become more pervasive, which is mainly due to three factors. Firstly, as discussed in Chapter 1, Iran is heavily investing into its Internet infrastructure. Secondly, Iran's youthful demographic is likely to make a relatively easy transition into the medium, especially since Internet use is heavily correlated with the age of the user, and most users with fixed access are in the age group of 18-28.[081] Finally, the penetration of mobile phones is already high at 79% and 60 million users, and further expected to grow, with mobile Internet access becoming more and more common for average Iranians.[082] The latter trend is also reflected in an estimated 4 million Android users[083] which are said to already account for 10% of the country's entire web traffic.

Yet aside from these rather indistinct numbers forming an incomplete empirical basis of research, other issues pertain to the quality of the data. Existing studies are biased towards male respondents: Iran Media Program's "Finding a Way", for example from 2011, consists of respondents who are overwhelmingly male (92%[084]). The operator of an online platform for Iranians sums up the exemplariness of this case: "We know there are a lot of women online in Iran, but what they do, where they go, we just don't have research on that".[085] A 2010 BBG study also seems to suggest that women in general are less often found online than their male counterparts.[086] Another bias, which

[077] / Non State: Small Media, Iran Media Program, Open Net Initiative, Freedom House. Private: Mainly telecom companies such as Mobile Telephone Networks, IGO: such as the ITU.

[078] / *Small Media Foundation (2013) – "Iranian Internet Infrastructure and Policy Report July- August"*

[079] / Ibid.

[080] / *Iran Media Program (2012) - "Finding a Way- How Iranians reach for news and information"* Data for the study collected via an international market research company which recruited a representative sample of Iranians. Interviews yielded 1022 completed questionnaires.

[081] / Ibid.

[082] / See for example *Freedom House (2013) - "Freedom on the Net – Country Profile: Iran"*

[083] / A number announced by Mahmood Liyaei, an advisor to the MICT. See *Small Media Foundation (2013)*

[084] / Which only seems to indicate that the men are prevalent on the downloading platform onto which the study, a downloadable survey had been placed.

[085] / TFI Workshop, August 8-10, 2013.

[086] / When asked whether the Internet has been used yesterday, 15% of female vs. 25% percent males were answering in the affirmative. See *BBG/Gallup (2012) - "Research Series Briefing: Iran Media Use"*

seems prevalent in studies, is the one towards urban environments to the detriment of rural areas, a distribution which nonetheless coincides with an estimation of a much less developed rural Internet infrastructure. Users generally live in one of the big urban agglomerations Tehran, Shiraz, Mashdad, Esfahan, and Tabriz.[087] Unsurprisingly, this population thereby also coincides with a particular socioeconomic status: urban and upper middle class dwellers to this day remain those being most capable of affording the still prohibitive pricing of the Iranian Internet companies who appear to be sharing the burden of their government's security driven governance of the Internet infrastructure.[088] The finding that Internet users to date include a large number of university educated citizens further reinforces the apparent specificity of social user milieu of the medium.[089] The extended Internet access is thereby not matched with research capturing large and growing sections of rural and female users, as well as those for whom socioeconomic status has thus far prevented access to the medium.

## *The Fall of Blogestan?*

Previous research has repeatedly conveyed the image of a particularly active Iranian user that produces and shares content online. This attribution has been mainly sustained by the fact that Persian had for some time constituted the second most used language in the blogosphere and accounted for a total of more than 60.000 regularly updated blogs.[090] More recently, however, a decline of the medium appears to have occurred, compared to the role it played in the years prior to the 2009 contested presidential elections. Although this alleged trend has not yet been substantiated, several close observers and experts on Iran's social media environment that we have consulted expressed a similar assessment, leading some to even conclude a "death of the Persian blogosphere".[091] The reasons for such a development could be manifold, ranging from the chilling effects of harsh government crackdowns[092], online surveillance and resulting self-censorship, to the global trend of an emergence and popularization of micro-blogging and social networks to the detriment of traditional blogging among Persian users. On the other hand, a study conducted in 2012, measuring the responsiveness and "freshness" of censored blogs identified a considerable number of blogs that were not abandoned even after being blocked, concluding that Iranians are "blocked yet blogging".[093]

This expressiveness of the Iranian user must meanwhile not be confounded with overly political contributions. At the time of the IMP study, even during the 2011 contestation and political uprising of the parliamentary elections and with a particularly young sample, politics did not top the agenda of users who preferred personal and scientific issues.[094] It remains unclear whether this finding reflects a general lack of interest or apathy in issues relating to politics, or whether it can be attributed to the chilling ef-

[087] / *Freedom House (2013)- "Freedom on the Net – Country Profile: Iran"*

[088] / See Part 1 Chapter 1 on Iran's National Information Network

[089] / *Iran Media Program (2012) - "Finding a Way- How Iranians reach for news and information"*

[090] / *Kelly, Etling (2008)- "Mapping Iran's Online Public: Politics and Culture in the Persian Blogosphere"*

[091] / A statement of participants of TFI's 2013 Berlin workshop.

[092] / See for example *DW (2012) – "Iran arrests wave of bloggers"*

[093] / *National Web Studies (2012) - "Mapping Iran Online"*

[094] / *Iran Media Program (2012) - "Finding a Way- How Iranians reach for news and information"*

fects of online surveillance. Users are thus likely to be aware of the potential threat that is posed by their government.[095]

## *Circumvention Culture*

Both quantitative research on Iran[096] as well as the public, official discourse inside the country indicates the existence of a *culture of circumvention*: A 2011 study, found that a majority of users (79%) admitted to being familiar with circumvention tools, of which half (51,5%) found it easy to access and to find such tools.[097] In the discussion on Iran's circumvention landscape, VPNs (Virtual Private Network) are usually referenced as having a large user base, generating an estimated 12 million dollar a year market.[098] This shows that, despite a generally tense economic situation and current high prices for household connections, Iranians are willing to pay additional amounts in order to obtain unfettered access. VPN use (and circumvention tools in general) has officially been declared illegal in public statements, which enabled officials to cut access to most such tools in the early onset of the 2013 presidential elections while offering officially accredited VPN services as an alternative[099] in order to respond to the demands of businesses. While private users consequently switched to alternative circumvention tools like Psiphon, Freegate, and Kerio VPN[100], government-vetted VPN services failed to attract private companies, which led to the termination of the "legal" VPN project.[101] Research furthermore indicates that a large share of users feels unsafe while making use of circumvention tools that are accessible to them.[102]

The difficulty of obtaining access may, however, come with a beneficial side effect, which is the relative technical sophistication and savvy of the Iranian user. This impression is further reinforced by the ability of Iran's online community to react both creatively and resiliently during government crackdowns on circumvention software, as indicated by the adoption of uncommon circumvention services in the run-up to the 2013 presidential elections.[103] On the other hand, researchers have repeatedly pointed out that the increase in demand for working circumvention tools "has not been matched by due diligence on the tools being used or the manner that people are obtaining them."[104]

It is furthermore worth mentioning that Iranian circumvention culture is a fragment of a wider context where culturally repressive policies have created an audience for a parallel media sphere with popular satellite formats such as BBC Persian and VOA[105]which remain powerful symbols of public discourse. Walking through Teheran, one cannot disregard the discrepancy between the official ban on sat-

[095] / *Anderson, Abadpour (2012) – "Fights, Adapts, Accepts: Archetypes of Iranian Internet Use"* A 2012 qualitative study, using pre-selected user milieu representatives (so-called archetypes) in order to acquire an understanding of user behavior. In the study, the majority of users was conscious of surveillance and therefore practiced self-censorship.

[096] / *National Web Studies (2012) "Mapping Iran Online"*

[097] / *Iran Media Program (2012) - "Finding a Way- How Iranians reach for news and information"* The information is taken from a second part of the survey, a self selecting sample of a questionnaire distributed via a popular file-sharing platform targeting Iranian youth.

[098] / *ITNA (2013) "Users spent 12 billion Toman for VPN services"*(Farsi)

[099] / *Small Media Foundation (2013) – "Iranian Internet Infrastructure and Policy Report July- August"*

[100] / See part 2 chapter 1

[101] / *HeraldBoy (2013) - "Iran Decides not to Pursue 'Legal VPN' Project"*

[102] / 41% according to *Iran Media Program (2012)*

[103] / *https://twitter.com/CDA/statuses/331370662058930176*

[104] / *Small Media (2013) - "Iranian Internet Infrastructure and Policy Report"*

[105] / BBC Persian according to an internal study reaches one in ten Iranians. See *Iran Media Program (2012)*

ellite dishes and their hardly hidden omnipresence. It remains therefore difficult to quantify how a suchlike environment with its profoundly ambiguous media usage shares and interprets information through informal networks of personal connections and word of mouth[106], or with the help of widespread “small media” such as Bluetooth[107], all of which remain important means of trusted communication within Iranian society. Such networks can be assumed to exist *especially* within young urban subculture (which is a significant portion of society: 55% of the population are under the age of 30, while 71% live in urban areas[108]), where the strife for access to uncensored information blends with a general defiance against authority.[109] This young and educated segment of the population is also especially responsible for the enthusiasm and quickness with which Iranians are adapting to new trends in communication technologies, mobile applications like WeChat, What’sApp or Viber[110] (all of which are, or at some point had been blocked by authorities). Similarly, Iran is currently identified as one of the growing markets for smartphones[111] like Apple’s iPhone which are extremely popular among Iranian users and in high demand despite their still prohibitive prices[112] and their limited updateability (and therefore usability) due to the sanctions regime.[113]

## *Emerging Netactivism and Developer Scene*

The strong ties and social networks characteristic for Iranian society clearly have, despite the risks users are taking, transferred onto the virtual realm where Iranians are using a multitude of formats (Facebook, Google+, FriendFeed, Twitter, Balatarin or Instagram). A 2013 syndicated study of the Dubai- based company Conovi[114] witnesses a similarly strong growth in the popularity of social networks for Iranians. Recently, a growing number of high ranking politicians have made use of Facebook and Twitter accounts, fueling a heated controversy about the legitimacy of foreign based applications and a growing divide between those opting to liberalize communications and those against it.[115] Meanwhile, 2013 had seen remarkable examples of the use of social networks for addressing concrete social and community concerns. These examples have proven social media’s ability to facilitate community organization such as witnessed by a campaign of Iranian Sunnis against the powerful telecommunications company Irancell, which managed to publicly jeopardize the image of the corporation and thereby force it to issue a public apology for remarks deemed offensive- despite powerful shareholders.[116] Another example of the potential power and impact of an increasingly social network-connected

[106] / ibid. finds that “strong ties” of interpersonal contact are still considered the most important source of information to many respondents (51%), even “weak ties” (28%) are still considered more important than the Internet (26%).

[107] / Ibid. Rougly half (48%) reported having sent or received content through Bluetooth.

[108] / *AlArabya (2012) – “Iran young, urbanized and educated population: census”*

[109] / *Kamangir (2012)- „Booze, Drugs, and Blogs”*

[110] / All of which are, or at some point have been blocked by authorities. See for example *gizchina (2013)- “Popular messaging app WeChat banned in Iran”*

[111] / *The National (2014) – „Middle East does like its smartphones“*

[112] / *Cnet (2012) – “iPhone 4 sales in Iran”*

[113] / See Part 2, Chapter 5

[114] / *Tfour.me (2012) - “Over half of Internet users in Iran use Facebook”*

[115] / See for example *Rferl (2013)- “Iranian Culture Minister Again Defends Facebook”*

[116] / *ASL19 (2013) - “Iranian Sunnis Responsible for Successful Social Media Campaign Against Irancell”*

Iranian public can be found in a recent campaign which organized citizens against environmental pollution caused by lead factories in Zanjan and Arak in Northwestern Iran.[117] Although such organization proves the continuing willingness and, given the possibilities of repression, audacity of citizens to organize via online platforms, it must nonetheless be conceded that these examples provide only minor political decisions which may still be altered by harsher government reaction. While events such as these provide snapshots of the potential role social media and new technologies could play for social dynamics, the increasing visibility of a growing tech- and developer scene outlines another stakeholder group that could impact future developments in this realm. Due to services like the locally developed online app store Café Bazaar, which is said to be responsible for 2 % of the entire network traffic[118], and the shortage of international offers, local app developers have managed to establish themselves as the creators of localized applications and services, such as the Persian Android operating system Farsitel.[119] Emerging formats like the conference series Ted x Teheran or the Startup Weekend[120] are witnessing the formation of a technology-affine section of the population which has a natural interest to participate in today's globalised information economy.

[117] / *Iran Media Program (2013) - "Persian Cyberspace Report, August 1st-15th, 2013"*

[118] / *Small Media (2013) - "Iranian Internet Infrastructure and Policy Report (2013) "*

[119] / http://farsitel.com/en/

[120] / The acronym *TEDx* stands for a series of globally organized conferences on the subjects of Technology, Entertainment and Design; *Startup Weekend* is a Seattle based format aimed at supporting and connecting tech-entrepreneurs.

The franchise, US-originating, and global-reach character of the events indicate the significance of this development.

# 2

## Basic Assumptions on Internet Freedom Policies

« content

Since the second part of this report is dedicated in its entirety to help alleviate the restrictive nature of Iran's online environment through the refinement of individual measures and policies, one cannot avoid a consideration of the regular practices of the Internet freedom community. This community consists of the various institutions and individuals who dedicate their time to assist Iranians in gaining access to free and uncensored information. Certainly, depicting a field consisting of multiple individual efforts and rather loose associations in a totalizing manner risks making generalizations, yet at the same time allows one to realize tendencies and extract learning experiences which can serve as guidelines for future policies.

Internet freedom initiatives are habitually based upon a common set of implicitly expected cause-and effect relationships - assumptions on how we expect the initiatives to bring about positive change in the targeted societies. These assumptions are set to influence policy makers', activists', and developers' behaviors, discourses, and investments. Outlining the basic underlying assumptions in the field could help to scrutinize their suitability and efficiency with respect to Iran.

A somehow similar effort has been undertaken by Ethan Zuckerman, director of the MIT Center for Civic Media. Zuckerman offers three answers by outlining a set of three prevalent "theories of change"[121], implicit assumptions on how Internet freedom initiatives are expected to take effect in closed societies. He considers these theories of change to be underlying and guiding the quasi-totality of means for the promotion of Internet freedom, although it is rarely explicitly stated. Zuckerman mentions the suppressed information theory, the Twitter revolution theory, and the public sphere theory.

The suppressed information theory assumes a generally strong and revolutionary effect of uncensored information which enters a repressive nation from its outside. Disseminating and providing access to otherwise suppressed information therefore leads to political change, spearheaded by political activists, and facilitated by existing domestic grievances.

The Twitter revolution theory maintains that the provision of systems that allow for rapid communications between citizens in closed societies allows for the unification of forces and the coordination of political action. This theory has become popularized by a series of media articles drawing a direct connection between applications such as Twitter and Facebook and the 2009 contestation of the Iranian elections, as well as the uprising subsumed under the Arab Spring banner.

The public sphere theory holds that communication tools may not lead to an immediate revolution or overthrow of government but rather provide forums for discussion and spaces for free speech, which ultimately change expectations of society as a whole and creates subtle long-term impacts.

Meanwhile, at close scrutiny, the "theories of change" seem to be heavily focused on the facilitation of political agency and the amplification of political discourse as the primary mechanism through which Internet freedom initiatives are expected to contribute to societal change. In particular, the first two theories, the suppressed information theory as well as the Twitter Revolution theory, purport the vision of a political vanguard which is enabled to spearhead political change.

Consequently, these implicit expectations shape policies, discourses, and concrete initiatives prevalent in the field of Internet freedom. Whether highly publicized projects like "Internet in a Suitcase", conceptualized and prominently presented as a communications tool catered to the needs of

[121] / *Zuckerman, Ethan (2010) - "Internet Freedom : Beyond Circumvention"*

tech-savvy activists and dissidents in countries like Iran,[122] or projects aiming to channel in certain suppressed, politically relevant information to users inside Iran, or Western governments' high profile political use of online channels as a means of outreach to Iranian activists[123]: a prominent part of  Internet freedom related projects as well as the dominant discourse attached to Internet freedom are highly politicized.

Prominent Iranian researcher and blogger Arash Abadpour indicates that the fixation on the facilitation of political agency and discourse has contributed to a narrow perception of the Internet as a political entity, and complicated its use for other functionalities such as community development, concluding that the " [p]oliticization of the Internet by major players including Western governments, outside NGOs and the Iranian diaspora, have resulted in a skewed Internet presence" in Iran.[124] Consistent with this observation, multiple interviewees and workshop participants remarked that the great majority of Internet freedom related investments and outreach efforts towards Iran were preferentially tailored to resonate with political activists, dissidents and high-risk user groups. To exemplify the shortcomings of a suchlike limited scope, participants referred to Sattar Beheshti, a "low-level" blogger with no record of political activism, who, due to a critical post on his personal blog page, died in jail after he had been tortured. Participants described Beheshti as an "ordinary user", representing the strata of user-profiles "who are currently not addressed by our programs"[125] - in this case, the design and distribution process of digital security education and training.

The problem with depicting Internet freedom as, in essence, a technologically upgraded political agency, is not only that this conceptualization potentially disqualifies approaches that lack an immediate and obvious political dimension, but also that suchlike overtly politicized approaches do not need to wait long to obtain their responses from the countries implicitly addressed. In the case of "Internet in a suitcase",  Sobhe Sadegh, the weekly publication of Iran's Revolutionary Guards Corps, reacted by explicitly mentioning the project, denouncing those aiming to make use of  the peer-to-peer wireless mesh network as "subversive" elements[126], thereby facilitating an already ongoing  technological arms race. Furthermore, it is questionable if under the current circumstances the expectation is indeed warranted that facilitating politically motivated agency alone could yield the intended results, as the respective actors like political activists, bloggers and oppositional journalists  are subject to unprecedented scrutiny, online as well as offline, making it severely difficult for them to translate the capacities provided through Internet freedom programs into an expansion of social and political space.

These observations are in no way supposed to call into question the importance of support for dissenting voices and political activists who run the greatest risk. Also, the necessity of technological solutions for safe access and communication is beyond question, given the paralyzing measures with which the Iranian authorities violate both rights. Rather, this excursus is meant to focus attention on the possible blind spots of dominant approaches, as they

[122] / *NYTimes (2011) – "U.S. Underwrites Internet Detour Around Censors"*

[123] / *The Globe And Mail (2013)- "Ottawa backs using social media to boost Iran's dissidents"*

[124] / *Arash Abadpour (2013) - "Iran", in "Internet Governance. The quest for an open Internet in the Middle East and Northern Africa"*

[125] / Statement made at the Berlin workshop, August 8-10, 2013.

[126] / *RFERL (2011) – "Iran's Revolutionary Guards Corps Warns Against 'Internet in A Suitcase' Project."*

suggest limited paths through which Internet freedom and outreach efforts can contribute to positive change. Large audiences tend to be marginalized by current programs because they are simply not considered relevant, due to a too narrowly defined definition of agency.  Established visions of Internet freedom thereby tend to neglect relevant potentials where the inclusion of a hidden majority could become its true motor.

Meanwhile, Zuckerman does not mention another theory of change, the broad outline of which has surfaced in different discussions during our research.  On a descriptive level, it has been articulated as a need for efforts that could resonate with a larger and more diverse set of Iranian Internet users. This understanding suggests investments in projects that are capable of incentivizing a broader non-political audience to become involved in initiatives provided by Internet freedom programs. Such an encounter may be facilitated through the provision of online resources and interactions that are not primarily conceptualized and promoted with the ulterior motive of their usefulness for political action. In reaching out to and attracting the diversity of non-political user-profiles, Internet freedom initiatives are supposed to expand and diversify the coalition of interests seeking more open online environments. Whereas the first three approaches tend to focus rather directly on the politically significant locus of agency, actors, and discourse in order to effect change, the latter, rather indirect approach aims to foster the formation of enabling environments that are not political per se, but from where spillover effects towards openness can originate. As indicated above, a suchlike approach requires the broadening of the envisioned target audience of Internet freedom efforts, which in turn necessitates other trajectories than political activism.

And yet, all four “theories of change” represent different approaches that need not be mutually exclusive, but should rather be deployed complementary. In essence, each approach can be said to represent one of two broad Internet freedom strategies outlined by a recent RAND study, in which they could expand social and political space “either by maximizing the number of rank-and-file netizens (...), or by training a handful of agenda setters—bloggers, online journalists, and the opposition leaders—to become more sophisticated users of anonymization, circumvention, and communication technologies. The former strategy primarily focuses on broadening Internet freedom for all users, regardless of whether they will use their access for political purposes. The latter strategy deepens online mobilization and communication opportunities for a handful of motivated individuals who advocate political change.”[127] In light of learning experiences of the past, what has been roughly outlined as a depoliticized, broadened approach towards conceptualizing and implementing efforts appears to be the underrepresented facet of Internet freedom strategy in the case of Iran. In this respect, it would be helpful to complement approaches that seek to deepen online capacities for politically motivated audiences, with more investments in initiatives that could be more inclusive or address other relevant potentials. In the next chapter, we provide an exemplary account of how this approach could be translated from a conceptual level into a more tangible scenario, which can serve as a starting point for further debate on the design and implementation of Internet freedom programs in the case of Iran.

[127] / *RAND (2013) - “Internet Freedom and Political Space”*

As discussed in rather conceptual terms in the previous chapter, an underrepresented facet of the digital freedom discussion with regards to Iran is the creation of enabling environments which are not necessarily political in nature, but, however, could contribute to and facilitate the achievement of goals inherent to Internet freedom. In the following chapter (Part 1) we suggest approaches to outreach to Iranian users in order to exemplify the notion of enabling environments. These approaches take shape in the form of investments into a rapidly evolving tech- and startup ecosystem - a domestic marketplace of ideas where potential alliances and unaddressed potentials have been localized by our discussion partners, and from where important domestic contributions towards more open communications environments can be expected if addressed and engaged through adequate incubation measures. Furthermore, outreach is envisioned in the form of "non-adversarial" digital initiatives and offers that could reach beyond activist and politically motivated audiences and serve as door-openers to broader and more diverse communities, increasing the number of users who interact with each other and, through the initiatives, with the outside community of organizations that seek to leverage their influence for the improvement of Iran's online environment. In this respect, the following discussion must not be equated with the marginalization of efforts that could support Iran's activist audiences to improve sociopolitical realities on the ground. It should rather be read as a strategic response to past learning experiences and complexities encountered, seeking to explore possibilities that would augment the efforts of civil society concerned with the improvement and expansion of online capacities and spaces for Iranian users.

Along the same lines, the creation of enabling environments also refers to organizational features prevalent to the field of outside actors working on Iranian communications. Part 2 of this chapter therefore draws attention to the discrepancy between the status quo and potentials of the quality and quantity of interaction and coordination between outside stakeholders sharing the same priorities.

The themes of both parts of this chapter were subject of a lively discussion during the workshop conducted in August 2013.

## *Part 1: Possibilities for Outreach to Iranians*

### Discussion

To many actors, the use of online channels for outreach to Iranians inside Iran remains intimately linked to the amplification of dissenting voices and the facilitation of political discussions and agency. This perception coincides with the previously discussed conception of a "Twitter Revolution" which focuses on a vanguard of political activists. A recent online initiative by a Western government illustrates this approach by aiming to reach out to activists "in the cloud…in Google Hangouts…on Twitter…and on Facebook" [128] to discuss the prospects of political change inside Iran.

Without being judgmental on their political nature, overtly politicized usage of online fora as a mode of outreach to Iranians certainly create chilling effects on the fora themselves. They tend to set the tone and framework in which the Iranian states' cost-benefit-calculations regarding the Internet and new technologies are overshadowed by the dominant narrative of political destabilization, which, sophisticatedly exploited by propaganda and security organs, reinforces antagonistic Internet discourses and trig-

[128] / *Address by John Baird at the Global Dialogue on the Future of Iran (2013)*

See also *The Globe and Mail (2013) - "Ottawa Backs Using Social Media to Boost Iran's Dissidents"* gers a tighter grip on online channels. The domestic propagation of the narrative of political change instigated by foreign entities through the use of online platforms influences the attitudes of Iranian users and acts as the interpretive filter through which outreach initiatives are perceived. To a broad spectrum of users who do not use the Internet and new technologies primarily as a platform for political discussion or a tool for activism,   this filter can effectively act as a deterrent and exclusion criterion, preventing them from interacting with digital initiatives, or to make use of and benefit from information and communication capacities provided by Internet freedom programs. Most importantly, this dynamic creates chilling effects, limiting the ability of the Internet freedom community abroad to diversify channels of communication and to broaden the scope of addressees and respondents inside Iran beyond activism-oriented and politically motivated user-groups.

Consistent with the experiences of other workshop participants, an Iranian technologist encapsulates the troubles that the community outside Iran, working at the intersection of connection technologies, freedom of expression, and online security, has recently been facing when trying to enter into a dialogue and establish new connections to netizens inside Iran: “the over-politicized scene shies potential newcomers away”. Experiences of those active in the tech-community abroad have suggested that both the technology-interested Iranians who had all the qualities of positively influencing the communications environment in their country, as well as the majority of users who were primarily interested in keeping up with global technology and communication trends, at times perceive those working outside with suspicion, being hesitant to enter into a dialogue. This observation elucidates the importance of the narrative that inevitably frames any effort to connect to and engage Iranian users. In order to broaden the scope of addressees inside Iran, digital initiatives would have to make offerings, address issues, and be framed in a way that allow for their popular adoption, i.e. the participation of a broader set of users who would otherwise be alienated by overtly political connotations. On the other hand, reaching out to a broader and more diverse set of users was described as a necessity by workshop participants - most notably in order to attract and identify potential allies, where common interest structures could result in fruitful cooperation towards less restrictive and more inclusive communication environments, as indicated by a seasoned member of the diaspora community with years-long experience in the field:   “We haven’t really managed to bring new people to our field. The field is very limited. I feel that we need to do a better job in engaging a larger set of users inside Iran, and that should be around new projects.”

The formation of sustainable and vital online communities was furthermore mentioned as the most valuable impact projects entailing an outreach dimension could generate. To the diaspora tech- and civil society community trying to advance security and information flows, the task of engendering community structures and expanding their user base inside Iran involves multiple complexities and uncertainties: In addition to the obvious challenges presented by the Iranian state, organizations have to be responsive to ordinary shifts in communication trends and consumption habits of users, which is further complicated by the fact that users are virtually sealed off by an electronic curtain which allows only limited feedback. The uptake of a digital initiative and the subsequent effort of building and expanding an online community around it were therefore described as a “trial-and-error process”, an “experimentation with multiple variables” which would have to be probed in order to identify the right strategy. Above all, this process would require appropriate time spans. Against this backdrop, the oftentimes short-term focus of projects was discussed as an additional impedimental factor. The attendees of the TFI workshop observed what appears to be funders' fixation upon measurable deliverables within time spans which are tailored too brief to nurture long-lasting community building processes and to implement long-term visions: "The problem is that inside the scene there are only two year plans maximum". Organizations were oftentimes inclined to conceptualize narrowly defined projects promising rather short term, quantifiable deliverables, in order to increase the probability of being funded. In this respect, the logic of funding can be said to disincentivize the adoption of longer term perspectives on Internet freedom efforts towards Iran.

### Toward Improving Outreach

In light of the shortcomings related to the status quo of outreach policies, as well as the above described difficulties emanating from the situation, we hereby suggest all actors with the capacity to implement or help implement policy changes to consider the following recommendations:

Make technology the common thematic denominator of outreach and align outreach to the dynamics of the tech- and startup ecosystem. In light of past learning experiences, participants argued in favor of adapting a wider and less politicized approach to outreach, enabling them to focus on domestic milieus and potentials that can prove crucial in the quest for connectivity. Consequently, "reaching out to techies inside Iran" became one of the focal points of discussions, indicating both the groups of players and the thematic frame perceived as most promising for reaching out to and engaging key stakeholders within their circles. Participants unanimously described the wider technical community inside Iran - consisting of distinct actor categories such as tech start-ups, developers, journalistic and academic entities with interest in technology - as indispensable counterparts, given their vested, albeit apolitical interest in unfettered access, and their professional expertise necessary to contribute to that end, in their respective capacities. The statement of a participant mirrors the reasoning behind this approach: "There is an academic community with research interest in related issues, needing access in order to follow other academic research, there is a tech startup community needing access in order to innovate and connect to other entrepreneurs in the world, there are journalists covering tech-developments and the entrepreneurial landscape and so on. Supporting these entities and pulling interested actors together, you can create a community preoccupied with technology and access." In fact, the Iranian tech-scene, particularly the startup-ecosystem, has seen rapid developments in recent years, as illustrated by formats such as the Iran Web Festival[129] or the Startup Weekend[130], a global tech-entrepreneurship grassroots movement becoming increasingly popular across Iran, giving rise to incipient stages of interconnectedness of Iranian tech-enthusiasts amongst each other, as well as with their transnational counterparts. Against this backdrop and in light of this vital momentum, a shared interest in technology was described as the lowest common denominator that could serve as both a trajectory to reach out to a broader set of likeminded, important constituents, as well as a comparatively safe sounding board for exploring common concerns regarding digital access and security, and fostering critical deliberations thereon. In order to be able to connect to these actors, "discussions should be technology-driven, instead of political", participants mentioned. Though far from featuring characteristics of a viable ecosystem, the emerging tech- and startup landscape provides multiple links that organizations concerned with improving digital access and security can draw on. Reaching out to these distinct congregations and

[129] / http://iranwebfestival.com/en/

[130] / See for example *Start Up Weekend Mashad*, *Start Up Weekend Tehran* /, or *Start Up Weekend Isfahan*

consolidating an alliance of interests will attract stakeholders and foster domestic dynamics congenial to the goals of Internet freedom. Firstly, actors within this framework are particularly attentive with respect to changes in Internet controls and obstacles to connectivity, and the establishment of coalitions that reach into these communities could expand the situational awareness of diaspora civil society in ways that external research and monitoring simply cannot match. Secondly, due to their technical expertise, actors within this framework could build up on and augment technical assistance and contributions provided by external organizations, eventually putting forth indigenous solutions to challenges prevalent to Iranian cyberspace. Lastly, the formation of a vital tech startup ecosystem could create spillover effects to the benefit of Iranian cyberspace at large, and significantly raise the sociopolitical costs of government interference with connectivity.

Research and support domestic tech- and startup ecosystem. Although individual efforts to identify and connect to the aforementioned actors exist, suchlike efforts are still at an early stage and only consider a fraction of potential allies. Establishing an overview of actors and individual projects within the broader tech-and startup ecosystem constitutes a starting basis from where one could determine appropriate forms of outreach. Based thereon, incubating existing structures and projects was discussed as the best course of action. Given the complex political circumstances (i.e. sanctions) and the sensitivity of the matter in the local context, participants agreed that the concrete design of outreach and incubation measures will be determined by the political obstacles, and should pay utmost attention to the issue of legitimacy in order not to discredit projects and entities on the ground. Incubation would not even necessarily require direct economic support. Participants argued in favor of connecting and convening domestic actors from distinct communities with common interest in technology and access, assisting in getting new and innovative tech start-ups off the ground through infrastructural support such as hosting, providing required technical expertise, security audits and similar assistance. Supporting the development and interconnectedness of entities and projects within this framework and enabling the continuation of their operations through the range of available incubation measures is tantamount to investing in long-term, indigenous technical and sociopolitical developments towards improvement of communication circumstances.

Provide “non-adversarial” apps and online platforms. In a slightly different approach, participants also outlined the importance of developing and providing apps and platforms around non-political subjects, describing suchlike initiatives as being ideally “non-adversarial”. It was emphasized that these contributions would have to address topics and make use of avenues of expression and interaction within the boundaries of the politically acceptable, while at the same time expanding social space online and serving as focal points around which processes of community building could be initiated, attracting and establishing communication channels to communities that have so far been untapped. Firstly, participants emphasized the importance of “non-adversarial” apps and platforms, based on the assumption that those contributions would have the best prospects of popular adoption and increasing the number of rank and file netizens that interact with contributions provided by diaspora civil society. In light of the isolationist nature of Iran’s online environment, digital initiatives that appeal to and are used by large audiences could be considered as a gain in and of itself, regardless of their “mundaneness”, most notably because the resulting multiplication of links reaching inside Iran constitute a crucial asset for the community of outside organizations - an asset that determines their leverage to accompany and positively influence developments in Iran’s online environment. Secondly, participants emphasized that the provision of "non-adversarial" apps and platforms would allow outside organizations to comprehend mechanisms of engendering the formation of online communities around given topics. In order to figure out the regularities and variables that determine the formation of community-structures, discussions revolved around the consensus that organizations would have to "experiment with different topics that are relevant to different communities. We don't pretend to know what the recipe is, but it should be investigated in a way that is explicitly innocuous, far away from political topics, to understand the other hard parts of the problem before moving into the political sphere." Lastly, "non-adversarial" apps and platforms as a way to introduce more Iranian users to digital platforms and functionalities can increase the volume of online interactions among distinct social and user groups, and translate into a changed perspective on the role of technology and its optimal use for participation.[131]

Initiate a culture of long-term planning. Admittedly, the above described perspectives necessitate the reconsideration of existing time-scales of projects. Workshop participants suggested alleviating the shortcomings typical of short-term projects with a culture which is not afraid of embracing a rather long term focused planning. Such an approach enabled organizations to focus their support on oftentimes already developing and existing organic processes which would further the interdependency of Iranian tech-communities with the outside. Not only do such innocuous and non-political approaches generate trust, but they ultimately are door-openers for the creation of channels which Iranians could use for political activity if deemed desirable.

## *Part 2: Community Building Outside of Iran*

### Discussion

Community building outside of Iran refers mainly to the multiplicity of organizations working on Iranian communications as well as the wider Internet freedom and technical community, and the quality and quantity of coordination and interaction amongst entities.

The field of actors working to advance safe and uncensored communications inside Iran suggests a rather scattered scenario. Coordination and communication amongst stakeholders is sporadic and usually limited to concrete initiatives and occasions where different organizations join forces in a coordinated fashion to advance a narrowly defined matter. This has for example been the case with regard to the issue of sanctions, where concerted campaigning efforts contributed to the issuance of exemptions of digital devices for personal communications from the sanctions regime.[132] However, cooperation appeared to merely exist in the context of projects. Organizations and individuals of the field were rarely able to congregate for an exchange of experiences.

Workshop participants described this culture as incidental to the structure of the field, as the direct result of an environment which fostered a lack of exchange: "Relationships between organizations are set up as predatory. We all compete for funding, and there is no designated safe space for me to find out what organization X is really doing." The sensitivity involved in the line of work made trust building between different organizations a key factor and prerequi-

[131] / RAND Corporation's comprehensive study on the relationship between Internet freedom and the expansion of political space in repressive environments concludes: „ (...) [The] expansion of social space online may lead to the expansion of political space, even when netizens do not at first intend to use the Internet for political purposes. In Egypt, China, and Russia, political online mobilization grew out of nonpolitical uses of the Internet. (p.208)" from *RAND (2013) - "Internet Freedom and Political Space"*

[132] / *ICHRII (2013) – "Iranians' Access To Technology Now "Up To The Private Companies""*

site for the sharing of information - a resource that could only flourish when given appropriate and designated spaces for the exchange of experiences.

Referring to Iran-related Internet freedom projects, a participant emphasized the detrimental effect of such an environment: “In the case of outreach to Iranians we are all experimenting and cannot foresee the outcome. But we don’t recognize that as experimentations. If we adopted that mentality, we could actually sit down and evaluate what worked and what didn’t and benefit from that information as a community.” A hindering of a meaningful evaluation of initiatives was the result of the absence of willingness to “admit to and analyze failure”, which was perceived as irreconcilable with the logic of grant-making and funders’ expectations. Similarly, even where such evaluation had been conducted, very practical barriers made it harder for different organizations working in the same field to benefit from the lessons learned. Workshop participants remarked the absence of mechanisms and spaces which could help “to keep track of failure and to share information”, which is all the more important, given the experimental nature, volatile circumstances and variables Iran related projects usually had to cope with. The systematic and in depth exploitation of information and results would rarely grow from such circumstances.

The usefulness of evaluation was exemplified when a participant discussed the stagnation of a passed project that aimed to bring filtered content to Iranian users. In describing what he had identified as the main components that had led to the stagnation, valuable learning experiences on user behavior and consumption trends came to stand out.

Meanwhile, funding of Internet freedom projects appears to be heavily fixated upon the development of distinct tools and initiatives with measurable deliverables, marginalizing investments in the development of a sustainable ecosystem- by advancing the coordination between organizations, disciplines, and projects with shared priorities. Open Internet Tools Projects” bi-annual Circumvention Tech Summit (CTS) could be regarded as a much needed and promising first response, dedicated to inter-organizational coordination and knowledge-sharing. Remarking the lack of suchlike designated spaces is thereby congruent with the statements of the wider Internet freedom community: The summit’s reports bear witness to the recurrence of such a demand for exchange.[133]

TFI’s workshop has been exemplary in how the encounter between individuals from Iran related organizations, together with actors with important learning experiences from other countries, already provided important inspiration for Iran related projects.

Finally, congregations of organizations could have made greater use of synergy effects or prevented unnecessary doubling of efforts respectively, through better coordination. Only recently, two organizations of the Iran community provided a placid example of this shortcoming when they found out that they had been programming almost identical apps. Similarly, a participant remarked that he witnessed the launch of an expensive mapping platform as a fait accompli, which his own organization had spent important resources on half a year before and could have provided to the other organization completely free of charge. The examples accentuate how a simple sharing of information could have optimized the field’s scarce human and financial resources.

[133] / See for example *Open ITP (2012) “CTS II Report”*; *Open ITP (2013) – “CTS III Report”*; *Open ITP (2013) – “CTS IV Report”*

## Toward Improving Community Building and Knowledge-Sharing

In light of the various shortcomings related to the status quo of coordination and community building outside of Iran as well as the above described difficulties emanating from the situation, we hereby suggest all actors with the capacity to implement or help implement policy changes to consider the following recommendations:

Incentivize cooperation, create designated spaces of knowledge-sharing and exchange. If a multiplicity of actors and actions bears a disadvantage, then there would not only be the risk of obscuring responsibilities, but also of diluting efficiency. It appears evident that coordination and knowledge sharing is not just a theoretical issue, but could significantly increase the impact of individual Iran focused initiatives and entities contributing to Internet freedom related goals. The indicated shortcomings could be alleviated through the creation of incentives for cooperation, as well as spaces primarily dedicated to coordination and knowledge-sharing. Creating these spaces appears to be both feasible and necessary, given the manageable size of the field of Iran focused actors contributing to the matter at hand - while a failure to do so risks taking a toll on the efficiency of the overall field. Furthermore, there exists the need for a much more pronounced inclusion of Iran focused entities that are not part of the Internet freedom community, such as traditional human rights organizations and, most notably, Farsi language media outlets and international broadcasters. This appears all the more pressing, since both thematic and personal overlaps are already de facto existing. Digital access to, and security of information and communications transcend the boundaries of the technical community, and are of obvious concern to the work of media[134] and human rights organizations[135]. Both entities could help to raise the profile of developments in this realm, and to significantly scale up the reach of Internet freedom related initiatives, such as digital security programs. It is therefore necessary to exploit already existing entanglements and to explore synergy potentials. A starting point could be a common emphasis on the subjects relaying those organizations to digital freedom and security.

The tech-community, as well as the broader Iran focused community - such as advocacy and human rights organizations and private enterprises like media outlets - have accumulated rich troves of learning experiences which can increase results of Internet freedom initiatives significantly if consolidated and shared systematically. It is essential that funding entities recognize the importance of fora that are dedicated to the consolidation of these experiences and efforts, and incorporate their sustainable establishment and maintenance in their funding calculus. The Iran Cyber Dialogue[136], conducted for the first time in March 2013 on the sidelines of the Global Cyber Dialogue, can be cited as an exemplary step in this direction. Grounded in the idea of a multi-stakeholder approach, suchlike structures for regular exchange could evolve into a permanent mechanism, convening the bandwidth of Iran related entities in order to exchange information, best cases and failures, synergizing individual efforts, helping to avoid duplication.

[134] / See for example Part 1 Chapter 2. Also, on the creation of fake media websites and other threats to foreign based journalists, see : *Access (2013)- "One of These Things is Not Like the Other"*

[135] / For example the documentation of cases where Iranian users have become victims of the regime's online surveillance apparatus. See for example *Iran Human Rights Documentation Center*

[136] / *Iran Cyber Dialogue (2013)*

« content

Similarly, it is essential that Iran focused entities actively participate and inject their on-the-ground, contextual knowledge into the debates and fora of the wider Internet freedom and digital security field in order to allow for a customization of the latter's technical contributions (i.e. tools for access and security) to local conditions, but also to profit from solutions implemented in other parts of the world.

## Discussion

As noted in Part 1, Chapter 2, complementary to the blocking of content, tools and services, the Iranian government, with the help of affiliated communities and organizations, has adopted a much more offensive stance in its effort to shape the user's online experience. Symptomatic for this approach is a sharp rise in phishing, malware, DDoS-attacks as well as disinformation and smearing campaigns. The detrimental effect of this approach is further amplified by an environment in which personal computers and mobile devices run on out-of-date, often pirated operating systems and software, littered with security loopholes, predisposing Iranian users to all kinds of malicious attacks.[137] Furthermore, users are burdened with the psychological effect of uncertainty, distrust and fear, resulting from news items on large-scale spying campaigns against Iranian users[138] as well as the deliberate spreading of rumors, exemplified by reports on the alleged spying intentions of circumvention tool developer Psiphon.[139] Researchers and activists have consistently pointed out that Iranian users, notably activists, "have completely lost trust in [the security of] online services".[140] This interplay of facts and perceptions allow us to describe the Iranian online environment as hazardous, bestowing a significant portion of risk on online activities.

Accordingly, in conjunction with the provision of tools and initiatives aiming to ease access to information and communication, another approach towards Iran has been the provision of digital security training and material. The totality of digital security efforts can be divided in three main approaches, according to the modality of interaction between experts and trainees. In the first approach, organizations offer live-instructed online courses, asking users to register in advance in order to take part in the classes carried out on specific digital platforms.[141] In another approach, trainers convene with a designated group of users in order to provide in-person, face-to-face training. Thirdly, learning materials in the form of video and audio tutorials as well as written manuals are produced and provided on multiple platforms and websites, allowing users to learn autonomously in a do-it-yourself manner.

Currently, significant investments (both monetary and non-monetary) are allocated towards the implementation of in-person training, aiming to create environments where trainers and a designated group of Iranian users encounter each other face-to-face.

The personal encounter allows the trainer to acquire detailed contextual information on the activities of the user, the technical and political conditions under which he or she operates, and, based thereupon, the digital threats that he or she needs to mitigate. This process of "threat modeling" subsequently qualifies the trainer to derive digital security requirements that are tailored to the specific circumstances and needs (or "threat model") of the user. Threat modeling has unanimously been described as an indispensible work step of digital security training and education. In turn, the actual technical dimension of digital security training (e.g. which software tools meet the security requirements of the users' threat model? How to encrypt communications? How to anonymize web-browsing? etc.) has been described as a mere matter of form, given that there is no shortage of technical means for mitigating

[137] / Western software companies are hesitant to provide Iranian users with access to software and updates out of fear of violating US sanctions requirements. See Part 2 Chapter 4.

[138] / *Google Blog (2013) – "Iranian Phishing on the Rise as Elections Approach"*

[139] / *IRNA (2013) –* (in Farsi)

[140] / Berlin workshop, August 8-10, 2013

[141] / See for example *Tavaana: E-Learning Institute for Iranian Civil Society*

digital security threats. Accordingly, the overall goal of digital security education is to enable the user to self-sufficiently assess his or her situation and needs on an ongoing basis, and to dynamically adapt the necessary tools and behavioral patterns as required by ever changing circumstances and threats. The sustainability of this approach grants the user flexibility, as one participant has put it: "If he shares pictures of cute cats, he might not want to bother with strong security. That's fine, as long as he knows when he should protect what information against which adversary. Once you get that across [as a trainer], you can talk about more concrete aspects like how to hide your IP or secure your web-browser, for which he has lots of tools at his disposal."[142] The key to this understanding - and at the same time the biggest challenge - is less the trainers' one-time and static prescription of certain technical details, but rather the sustainable conveyance of how to think about digital security, resulting in the users' changed mindset, i.e. a basic awareness of the interdependency between digital tools and behavior and the exposure of information. In articulating the reasoning behind this understanding, a seasoned trainer stated that "we are trying to move away from this being a technical IT-problem, for which the user gets a one-time fix and then they think they are safe, as opposed to creating conceptual awareness of digital security so they are able to identify threats themselves and understand why and when they should use this or do that. So creating awareness is the first step but also the most challenging because you have to figure out how to engage the user." [143]

We have consulted with several experienced trainers who described this facet of training and education as a behavioral challenge, which in turn demands from the trainer some form of didactics, i.e. a consistent structure of the educational effort, and appropriate methods to engage the users' mind in order to affect behavioral change. As a result, there seems to be a growing consensus in the field towards a "school of thought" that conceptualizes and teaches digital security as a sequential process, engaging the user in order to create awareness for general concepts, and subsequently moving to particular technical aspects as required by the context of the user.[144] However, it is important to emphasize that not all trainers adhere to these insights, which in turn amounts to varying quality standards prevalent in the field of digital security training and education materials.

Against the backdrop of these educational goals, face-to-face trainings certainly present the proper setting, enabling the trainer not only to jointly carve out the users' threat model and derive customized security measures, but also to convey conceptual awareness for digital security and threats, leading to sustainable "digital hygiene".

On the other hand, personal face-to-face training is tied to certain limitations. Due to the associated efforts and costs, it is evident that -quantitatively- the range of beneficiaries could only be very limited. Another constraining factor is the small number of active members in the Iran focused digital freedom community who speak Farsi, and have the necessary qualifications to provide personal digital security training. It has been noted that there are enough potential candidates in the technical community inside Iran who could be engaged and trained to act as trainers, which would significantly simplify the process. But "they either don't know how to get involved, or they find it too risky", as one Farsi speaking trainer stated.

[142] / Berlin workshop, August 8-10, 2013. Emphasis added.

[143] / Berlin workshop, August 8-10, 2013. Emphasis added.

[144] / This growing consensus has been articulated during the Circumvention Tech Summit IV, hosted by the Open Internet Tools project in Berlin, where, drawing on past learning experiences, many seasoned and reputable trainers and training organizations clearly argued in favor of this „school of thought“. See also the summit‘s report: *OpenITP, Circumvention Tech Summit IV Report*

Adding to these quantitative constraints of in-person training, there are also qualitative deficiencies. Both Farsi-speaking and non-Farsi-speaking trainers pointed to the lack of means for assessing the efficiency and outcome of training sessions. Some trainers mentioned that there exist uncertainties on the suitability of training methods, how trainings are received, and whether they are implemented by the user, with one seasoned trainer stating that "we are sort of fumbling in the dark on what we think is right." Another trainer of Farsi speaking users explained: "It is this culture of flying them in for three or four days, going through all the security issues, and after that they think they are secure, we think they are secure and then good bye. But we actually don't know. We need to follow up on them, but we don't have the capacity for that."[145] Consistent with this observation, participants referred to the lack of empirical research data that could be used to carve out more accurate representations of threats in Iranian online environments, thereby substantiating the working assumptions in which trainings and education materials are grounded on. In the case of Iran, essential details on the state's actual capacities and procedures with which they compromise user security are in great parts still ill-defined, due to poor documentation, as a technical expert on the issue has pointed out. Deliberate spreading of exaggerating accounts on the state's capacities amplifies ambiguities, creates widespread distrust and chilling effects on user communications. Multiple interviewees indicated that the detrimental effects resulting from the circulation of myths and disinformation on security issues is one of the most under-appreciated aspects in the discussion on Iran.

Further limitations of in-person training are tied to the composition of the group of beneficiaries, as it consists almost exclusively of high-risk users like dissidents and activists. This observation is understandable, given the increased security needs of activists' digital communications and online activities. The limited scope of addressees that can be targeted by in-person training initiatives makes it all the more important to compensate these limitations by systematically expanding the other modalities of digital security training in order to reach broader audiences.

The creation and dissemination of digital security resources for autonomous learning is yet another method of delivering training and education. The educational goals striven for during in-person trainings as noted above are certainly harder to achieve and convey due to the absence of direct interaction between trainers and users. Therefore it is all the more important that the preparation of educational resources happens in due consideration of these goals.  In this respect, when creating online resources, leading innovators specialized on digital security education increasingly place value on appropriate didactical methods, using appealing, easy to digest formats to facilitate conceptual awareness for digital security, accompanied by manuals that guide the user through a subsequent deeper examination of concrete, technical  issues.[146]  In relating to this rationale, workshop participants stressed the qualitative difference between mere recommendations on isolated aspects of digital security, and education on the underlying regularities that determine security and privacy, the latter of which is more likely to affect  sustainable behavioral change: "If the user doesn't understand how and why a certain tool or behavior negatively affects his security, then it is even harder to convince him to move away from it in the long run."  Just like with in-person training, online resources that follow a process-based ap-

[145] / Berlin workshop, August 8-10, 2013

[146] / See for example Tactical Tech Collective's animated films and online-persona, through which they creatively conceptualize digital security and threats by embedding them in comprehensible narratives and games: *https://myshadow.org/* data-dealer and *https://onorobot.org/* . *Tactical Tech's "Security in a box"* in turn provides more concrete technical manuals and hand-on guides to tools.

proach, guiding the user from general concepts to particular aspects, promise holistic and sustainable education results.

Meanwhile, online education resources in Farsi exist in high numbers, produced by various actors and organizations. Given the multiplicity of actors involved in content production, it comes with little surprise that providers adhere to different standards, and resources are therefore produced based on different understandings on how to educate users on the complex, technical and multifaceted subject of digital security. A lack of producers' awareness of other existing curricula, as well as cooperation on development, but also a lack of funder coordination could be perceived as leading to a high diversity of material.

Farsi content mainly exists in the form of audio-and video-recorded lectures and written articles, by which the vast majority of providers elaborate on specific partial aspects of digital security in a rather unorganized sequence, lacking a thought-out didactical strategy capable of structuring the overall task. Regarding design and didactics, there seems to be a qualitative gap between the cutting-edge techniques and insights applied by actors like Tactical Tech, and the bulk of available Farsi content. Some resources like awareness-raising animated clips have been translated into Farsi. Nevertheless, as geographically non-customized online resources seek to address a global audience, they can only insufficiently yield to specific local "digital" and cultural conditions and peculiarities under which Iranian users operate.[147] The isolated examination of select aspects in Farsi education materials clearly has a practical value, as it prescribes and recommends a fix to a problem, i.e. a digital threat. Still, there are only few Farsi resources that are sophisticatedly composed in order to actually guide the user through a reasonable education process - grounded in the above mentioned school of thought that we have come to learn as most promising. Instead, the user is constrained to embark on a paper chase, sourcing education materials that are dispersed on multiple websites and platforms. Furthermore a great deal of digital security resources is provided by sources and platforms thematically oriented towards either politics and activism or digital culture[148], often times conflating both realms.  Accordingly, the current arrangement reaches user profiles that operate in those realms, and therefore quite possibly have some form of rudimentary awareness for digital threats and personal security needs, or a vested interest in related topic areas, like political and social activists, journalists and tech-savvy users. Iranian users that are neither in line with the collective profile characterizing this sample nor active participants of this ideational and communicative ecosystem, are insufficiently covered by the current configuration of the marketplace of digital security resources and discourse. However, the urgency to expand the scope of this arrangement arises from the conjunction of multiple circumstances.

Iranian users' awareness level for digital threats and personal security needs varies, with some being security-minded, sensitized through their professions and activities that require delicate handling, and the majority, with rather "mundane" user profiles, being little appreciative of (i.e. knowledgeable) modalities of security and privacy.
While in theory the congruence of activity profile and se-

[147] / It is for example a common practice in Iran to go to a random shop selling consumer electronics, for example in the bazaar, and leave one‘s mobile phone or tablet with the shopkeeper, who then installs a range of often times pirated applications and software - with considerable security implications due to malware.

[148] / See for example *Balavision*, featuring discussions on politics and democracy, *Tavaana*, focusing on capacity building for social and political activists:, its digital security arm *Tavaana Tech*, or *Technevis*, providing news on technology and digital culture. All sources provide material on digital security.

curity awareness and -needs might be reasonable, in practice, present-day socio-political dynamics in Iran make such a categorization far more complicated, as one workshop participant has explained: “It’s a very thin line in Iran between being an ordinary citizen and becoming a person of interest or an activist. It can happen overnight. It’s not like in other countries where being an activist is a profession, where you know you have to learn basic necessities. It is very common in Iran that, on one day, you do regular stuff, and the next day you become activated, cross a line without having the proper awareness for digital security.” Participants agreed that this sudden shift between different categories of need for digital security, caused by the users’ changed online activities, is seldom met by a corresponding awareness for that need, thereby making the case for reaching those user-profiles who are not the “typical” addressees of educational offers. Apart from such cases, where newly politicized individuals underestimate digital threats, even established activists may, despite their own enhanced and careful precautions, be exposed to risks generated by the activities of their relations. A well-known security rule of thumb states that every network’s security is only as strong as its weakest link, and therefore serves as a reminder that even an individual’s careful personal activity is challenged by risk outside of her capacity of control.

The same call can be derived from the undesirable side effects of the struggle for access. The need to establish access to the global Internet is a permanent, day-to-day challenge - logically not only faced by activists and dissidents, but by the great majority of user profiles seeking an unfettered connection. The struggle to satisfy the need for access not only marginalizes digital security as an issue. To a certain degree, the compromise of security becomes a requirement in order to satisfy the need for access, as a prominent Iranian blogger explained: “As an Iranian, you literally have to accept the fact that you have to compromise your security if you want to communicate. The process is so complicated, it almost leaves you no choice. You try this VPN, it doesn’t work, then you try this circumvention tool which you have heard of, but you have no idea how it works or whether it is infected, and then you might have to install this other plug-in. And every step on your way means a compromise of security, especially for those who are not experts.”[149]

## Toward Improving Digital Security Education

In light of the various shortcomings related to the status quo of digital security training and education, as well as the above described difficulties emanating from the situation, we hereby suggest all actors with the capacity to implement or help implement policy changes to consider the following recommendations:

Refrain from linking digital security education and discourse to political and social activism in order to be able to reach the “ordinary” user. Tellingly, an Iranian trainer and activist abroad working closely with activists inside Iran, stated that “we should move away from how to protect an activist to how protect your password. Because everybody benefits from it if we tell them how to protect your passwords.” In an increasingly networked population, the issue of digital security should be approached in a more holistic manner. Resources targeting at risk-users like activists and journalists should be complemented by more investments in initiatives that address the activity profile of the “ordinary user”. In order to popularize digital security among Iranian users and to relate to users who are uncomfortable with using materials that have a political framing and are geared towards activism, education materials should be produced in as neutral a language as possible.  Curricula could be grounded in the narrative frame of cybercrime,

[149] / Interview, October 19, 2013.

linking digital security education to the trend of e-business and e-banking , which will gain importance in light of increasing Internet penetration rates , the looming National Information Network and publicized high-profile cases of online fraud inside Iran.[150] A de-politicized approach to digital security will facilitate the opening of new channels, through which education material could reach the Iranian end-user. Similarly, the following propositions should be considered under this aspect.

Create integrated and cohesive Farsi curricula for autonomous learning. There exists a wide range of articles - usually in the form of news items or blog entries - as well as online videos explaining select aspects of digital security, like password security or online anonymity. These efforts should be complemented through the creation of more comprehensive resources. Curricula should guide users through a sequential process, moving from facilitating awareness and understanding of fundamental principles of digital security to guidelines on the practical application of its multiple facets. Particular focus should be laid on addressing and appealing to users with limited technical skills. It appears not necessary to reproduce topical subsets that are already available in other resources and still relevant and up-to-date. Instead, they should be adjusted according to the target audience. Iran experts and dedicated training and education organizations should join forces in order to harness the former's detailed knowledge on local technical, political and cultural circumstances to the latter's advances and cutting-edge insights in didactic methods and means. This is to ensure that Farsi curricula keeps pace with the evolving consensus in the wider field of digital security education on standards and best-case approaches, and at the same time is customized to local circumstances.

Re-assess and produce digital security curricula in due consideration of the implementation of the National Information Network (NIN). The NIN not only emphasizes the urgency of digital security education for a much larger group of addressees. The working assumptions on which education resources are based upon need to be aligned with the fundamental technical changes associated with the NIN.

Make available and market education resources in a way that ensures that they are reachable by and receive the attention of a wider spectrum of users. The communicative spaces currently hosting digital security resources and discourse strongly privilege users who have an intrinsic interest in activism or tech-culture, missing out the diversity of users with different patterns of online behavior and motivations. Providers should expand and relocate outreach and visibility to spaces and platforms with as heterogeneous an audience as possible. Providers should explore different collaborative arrangements with Farsi language media organizations, leveraging their reach to cast a wider net and extend the scope and scale of addressees, which will be essential for the effort of truly popularizing digital security as an issue. One interviewee involved in the creation of curricula exemplified this approach: "There are excellent animated short films on digital security, natively translated into Persian. Why don't we for example share that with broadcasters? It is unnecessary to write about how SSL works for the fiftieth time. Why don't we consolidate the good material and come to an agreement on how to distribute them? Everyone stands to gain if we consolidate processes so that we have a multiplier effect for our investments." As indicated by the interviewee, a drive towards a consolidation of resources and distribution methods will - as a concomitant feature - ultimately have a narrowing effect both on the variation in quality and the dispersion of efforts. This requires better coordination be-

[150] / *ZDNet (2012) "3 Million Bank Accounts Hacked in Iran"*

tween producers as well as funders of digital security resources.

Use appealing and easily digestible formats that are suitable to attract the initial attention of a broader audience. Certain selected aspects that feed into the overall task of digital security education should be formulated and presented along the lines of outreach and awareness campaigns. A suchlike campaigning approach can be used to debunk and correct the most prevalent misperceptions and disinformation on issues relevant to digital security in Iranian cyberspace, while at the same time serving as a teaser that entices the average user to make use of more expansive educational resources. Campaigns should also draw on real life examples users can relate to, and outline the consequences of compromised digital security. This outreach or "marketing" oriented dimension requires a concerted approach that utilizes foreign based Farsi language media as well as other platforms with large audiences inside Iran.

Put digital security on the internal agenda. Media organizations for which digital security has so far been an off issue should place value on internal alignment of staff's digital behavior through awareness raising and continuous educational initiatives. While more and more foreign based Farsi language media outlets have taken measures to protect their digital infrastructure against DDoS and similar malicious attacks, the communications security of individual journalists and staff members has evolved into a preferred target. Given the interconnectedness of foreign based journalists and users and sources inside Iran, a compromise of journalists' digital security simultaneously puts Iranian users at severe risk.

Train the trainers. There exists a lack of Farsi speaking trainers which should be addressed through the training of trainer's initiatives. The instruction should be conducted in a standardized fashion to guarantee that all trainers are equipped with the same qualifications, which, beyond technical expertise, should include a basic understanding of didactics as a prerequisite of effective education.

Create processes and capacities in order to follow up on trainees. Gained insights should be shared with other trainers and training organizations and used in order to refine and review content of curricula and methods of training. When compatible with security requirements, the collection of follow up data should be considered as part of the training initiative. Furthermore, trainers are ideally positioned to learn about Iranian end-users' adoption of and approach to "Western-built" circumvention and privacy tools. This information should be systematically collected and shared with developers and the technical community, so tools can be customized according to Iranian end-users' needs and usage patterns.

De-Brief political prisoners and users who have been confronted with their digital footprint (e.g. in the court of law or when being interrogated by security organs), or whose communications have been compromised in other instances. Empirical data should be compiled and evaluated in order to create more concrete representations of the actual technical capacities and procedures with which state organs compromise user communications, thereby substantiating working assumptions of digital security curricula and training. In order to ensure that de-briefs generate the granular technical specifics necessary for the task, they should be conducted according to standardized, expert-drafted questionnaires, which should be shared with organizations and NGOs active in the respective field.

## Discussion

The Iranian regime maintains one of the most wide-ranging and sophisticated Internet censorship programs in the world. For Iranians who are online, the utility of the Internet can in great part only be experienced through the use of censorship circumvention tools. In the following chapter we provide a framework that could help to evaluate the role circumvention tools have come to play for Iran's Internet population, the adoption and use patterns, and the barriers that compromise the users' circumvention experience. In doing so, we try to outline the use cases that are most common and may describe the experiences, motivations and perceptions of the "average user". This framework could therefore be helpful to determine the utility of circumvention tools that attempt to cater to the needs of broader audiences, and to identify the factors that correlate with the wider adoption of tools. By implication, this framework is not meant to be all-encompassing, as it omits the unique needs and concerns of the group of high-risk users.

In the concluding part of this chapter, we particularly draw on the operation of Psiphon3, a censorship circumvention tool available for Windows and Android that uses different protocols to connect users to the uncensored Internet.  Our focus has been based on the circumstance of having been granted insight into the working and learning process of Psiphon's team, as well as insightful research on Psiphon3[151] usage in Iran, which has been published by researchers at ASL19.[152] Due to the popularity of Psiphon3 among Iran users[153], we furthermore believe that the example holds valuable lessons with respect to the aforementioned scope and intention of this chapter.

Given the difficulties involved in conducting surveys in repressive environments, research contributions that aim to establish a representative overview of the size and type of audience that uses and depends on circumvention tools are heavily constrained. Although limited with respect to the specific issue of circumvention, Iran Media Program's (IMP) 2012 conducted study on Iranians' media use and communication habits can be regarded as one of the most reliable, due to its methodology[154]. In a field survey that was carried out, based on a systematically recruited sample of Iranians which mirrored the demographics of the country, 44 % of Internet users reported that they would either often or always encounter blocked websites when they were online. 26,5 % said they were familiar with tools that help circumvent blocked websites. Although interviewers used hypothetical language to mitigate the respondents' discomfort that might arise in a face-to-face conversation with a stranger on the issue of circumvention, the authors conclude that "[t]he actual number of people familiar with the existence of circumvention tools is almost certainly much higher among internet users in Iran."[155] Unsurprisingly, it was the younger respondents who reported their familiarity with circumvention tools. In a second IMP survey which was hosted on the 20th most visited website in Iran, which, at the time of the survey was not filtered, 79 % of the 2802 respondents declared their familiarity with circumvention tools, while 51,5 % said it would

[151] / See *Psiphon3*

[152] / See *ASL19*

[153] / *November 2013 statistics indicate the number of 800.000 daily unique users for psiphon 3*. According to privately shared data, this number has by now surpassed 1 million daily unique users.

[154] / *Iran Media Program (2012) - "Finding a Way- How Iranians reach for news and information"* Interviews yielded 1022 completed questionnaires. Questions were worded in a way that would ensure the safety of respondents, as well as the likelihood of answering honestly.

[155] / Ibid. p. 24.

be either easy or very easy to find and access such tools.[156] Over 80% of respondents to the online survey were under 30 years, which, given the demographics of the general population, lends additional significance to the finding.[157] Aside from quantitative approaches that provide some indication of the potential size of circumventing audiences, qualitative research adds to the picture by outlining the type of audience that uses these tools and, by implication, the diversity of motivations for doing so. Abadpour and Anderson’s  2013 published study “Fights, Adapts, Accepts: Archetypes of Iranian Internet Use”[158] establishes different unique user profiles (archetypes) based on Iranian users’ varying online habits, attitudes, and relationship to the Internet, a methodology which “is meant to qualitatively describe an inclusive set of models that attempt to cover the general population of Iranian Internet users”[159]. In-depth interviews with representatives of these 18 archetypes allow the authors to conclude that, spanning across the range of distinct user profiles, “respondents nearly uniformly state that they actively bypass systems of Internet control and filtering”.[160] The authors’ findings pointing to the “commonplaceness” of circumvention practices “in the daily habits of the general public” indicate the existence of circumvention as a widespread practice.

If we follow these quantitative and qualitative findings, providers of circumvention tools seem to face a large and heterogeneous audience of tool users inside Iran. These findings also carry indications on Iranians’ motivations for circumventing online restrictions. Quite to the contrary of the above account, research performed by Harvard’s Berkman Center on Internet and Society on usage rates of particular circumvention tools indicates that only 3% of users in filtering countries make use of circumvention tools.[161] The authors hypothesize that, among other reasons, the low rate of tool usage could result from a lack of users’ interest in content that has been blocked. The low number of users, in addition to the poor performance of a range of circumvention tools tested by Berkman researchers, leads the authors to the conclusion that “focusing on building highly reliable, blocking resistant tools with fast throughput for a small audience of users might focus the attentions of software developers more precisely. We believe there’s some truth to Xiao Qiang’s idea that a small set of internationally connected activists can disseminate information through local networks. And we worry that efforts to reach very broad audiences with circumvention tools is trying to solve a demand problem by focusing on supply.”[162]

The arguments on user motivations and needs inherent in these deliberations seem to mirror a general tendency in the debate on the role of circumvention tools in filtering countries. The outstanding value and utility of tools to users tends to be ascribed to the ability to access particular

[156] / Ibid. p.35. They survey was uploaded to the filesharing platform www.4shared.com.

[157] / This additional significance should nonetheless not obscure the fact that the study is based upon a self-selecting sample, and thus can only claim a limited representativeness for Iran’s online  population in general.

[158] / *Anderson, Abadpour (2012) – “Fights, Adapts, Accepts: Archetypes of Iranian Internet Use”*

[159] / Ibid., p.5.

[160] / Ibid., p. 17.

[161] / However, the applied methodology is problematic, as the researchers do not interact with users, and instead rely on self reporting of tool developers, as well as on Google Insight and Ad Words to gauge the popularity of different tools. *Berkman Center for Internet & Society (2010) -  “2010 Circumvention Tool Usage Report”*

[162] / *Berkman Center for Internet & Society (2011) - “The Evolving Landscape of Internet Control: A Summary of Our Recent Research and Recommendations”*

types content that authorities have identified as threatening to social and political stability and therefore decided to filter. If the necessity to resort to circumvention tools would only occur to those Iranian users who seek access to that type of "objectionable" information, then the relationship between the lack of interest in blocked content and the low number of circumventing users - as suggested by the Berkman research - might be applicable to Iran. However, the dynamics of filtering and circumvention in Iran suggest a notably different picture.  The technical censorship apparatus put in place by Iran's authorities is considered as one of the most pervasive and wide-ranging to date.[163] The problem of collateral filtering is an inherent feature of Iran's multilayered censorship mechanism, whereby practices like keyword filtering lead to significant over-blocking, affecting the most mundane information and websites.[164] Therefore, simple online tasks like academic research or access to innocuous content that is not officially deemed "undesirable" by authorities can be subject to unintended blocking. The significance and ubiquity of collateral filtering is exemplified by research on Iran's censorship of Persian Wikipedia sites: "In all, researchers found a total of 28 blacklisted keywords (all but two being sexual terms) that blocked 92 Persian Wiki-articles, 31 of which were effectively misidentified as sexual or profane."[165] As one of our discussion partners who closely observes Iran's online environment pointed out, "whether or not you find what you are looking for can at times be a game of pure chance"[166] when browsing the Internet in Iran. In addition to the randomness of filtering which can potentially affect the surfing experience of a large and diverse audience, reasons for turning to circumvention tools also figure in online habits and communication patterns of Iranian users. A 2012 BBG/Gallup study[167] found that Google (62%) and Yahoo (44%) were the most visited websites in the prior week, and according to a recent survey, 58 % of Iranian Internet users use the blocked social network Facebook[168], while IMP's youth-survey finds that 68% belong to online social networks[169], most of which - just like Facebook - are either intermittently or permanently blocked. Data on the usage of Hotspot Shield, a VPN which is reportedly widely used in Iran, lends additional clarity: "In Iran, the most popular page accessed through VPN in January [2012] was, overwhelmingly, Facebook, followed by Google, YouTube and Yahoo", and "other sites accessed on the VPN suggest Iranians want to use the Internet simply to live their normal lives. The fifth most accessed site is a complex online game site called Travian, at which users can build virtual empires."[170]

In light of the aforementioned, it appears more than likely that encountering access restrictions is not an experience only made by those segments of Iran's Internet users who seek a particular censored content that has been classified as threatening or undesirable by the authorities. The present state of filtering and circumvention therefore affects a much larger audience, and thus also other online activities than consumption and production of "sensitive" content. In a report analyzing a pilot program the BBC conducted to provide web-proxy services to Iran in order to make its

[163] / *The Guardian (2012) - " Internet censorship listed: how does each country compare?"*

[164] / Misidentification of character patterns in the URL of a website or in search requests can trigger the filtering apparatus.

[165] / *Nima Nazeri and Collin Anderson (2013) - "Citation Filtered: Iran's Censorship Of Wikipedia"*

[166] / Interview conducted on October 25th, 2013.

[167] / *BBG/Gallup (2012) - "Research Series Briefing: Iran Media Use"*

[168] / *The Next Web (2013) - "58% of Iranians use Facebook despite blocks and censorship, study finds"*

[169] / See footnote 154.

[170] / *The Washington Post (2012) - "Iranians using proxy servers 10 times more than they were last year"*

blocked BBC Persian content available, the authors document, among other things, the number of page requests per login (the BBC Persian website was configured as the first landing page after following a proxy link). It is laid out that the BBC experienced an approximate average of 15 page requests per login through its proxy-node which was propagated to Iranians. However, "[t]his data takes into account all sites visited for each login. When looking at BBC sites only, the number of requests per login is far lower. On the BBC Persian site, looking specifically at requests from the target market (Iran or Unknown) from January to July 2011, the average number of BBC pages viewed is 2.2 per session."[171] The authors conclude that "[i] f the audience is willing to use the service to access sites other than the host's, then they are using the nodes as part of their everyday browsing experience (...)."[172]

Summarizing these insights, one may conclude that the role of circumvention tools in Iran reaches far beyond than just being a gateway to "forbidden" information, or enabling only politically significant information consumption.[173] Their significance and broad appeal stems rather from their widespread apolitical utilization for unrestricted access to everyday information on search engines or, perhaps most importantly, to online platforms and services for messaging and communication with colleagues, friends, and family members. The importance and prevalence of these instances of rather mundane online information consumption and interpersonal communication also shed light on the role of circumvention systems in the mobile context. In 2013 Iranian authorities have intermittently or permanently blocked a range of mobile online platforms and applications for messaging, networking and Voice over IP services.[174] As applications like WeChat, Viber, Tango and WhatsApp have managed and will continue to attract a significant number of users in Iran, assessments on the role and properties of tools that correlate with popular demands should factor in this continuing trend. However, even as the most common use cases in Iran suggest rather mundane information consumption and communication, in tightly controlled information environments the role of circumvention tools can change rapidly. In the aforementioned BBC case study, the authors point out that the number of proxy users quickly increased during events of political significance[175], indicating that users who do not employ circumvention tools on a regular basis turn to these systems and benefit from their availability at critical junctures and during news events. One may conclude that encouraging the widest possible adoption and circulation by providing tools that meet the requirements of the most common use cases is an effective preemptive measure to ensure the availability of tools to non-regular users during times of heightened information needs.

Another factor that should be taken into consideration pertains to the handling of the issue of circumvention in the local sociopolitical discourse and its implications for user attitudes and perceptions. As outlined above, the interplay

[171] / *Canada Centre for Global Security Studies and Citizen Lab (2011) - "Casting a Wider Net: Lessons Learned in Delivering BBC Content on the Censored Internet*"

[172] / Ibid.

[173] / A notable pattern in both the BBG/Gallup and IMP surveys is the predominance of TV as an information source, even among younger and technologically savvy segments. Most strikingly, besides satellite TV, Iran's state broadcasters figured prominently as a popular source of information.

[174] / *International Campaign For Human Rights In Iran (2013) - "Restrictions on Internet Access and Mobile Apps Grow During Rouhani Administration"*

[175] / *Canada Centre for Global Security Studies and Citizen Lab (2011) - "Casting a Wider Net: Lessons Learned in Delivering BBC Content on the Censored Internet"*

of the pervasive nature of Iran's filtering apparatus, the range of mundane, day-to-day online activities that are affected by it, and the emergence of communication habits and modes of social interaction that are digitally enabled , has created a large and diverse Iranian audience which has come to depend on circumvention services. This situation gives rise to questions regarding legality and consequences of circumvention which, according to observers, "Fatwas, Iran's formal laws and regulations do not fully clarify (...)".[176] Whereas the development and distribution of circumvention tools are formally forbidden, the Iranian governments' response to the use of circumvention tools can be described as tacit consent.[177] Legal enforcement has happened in the context of production and distribution of tools or based on online expression and activities challenging state imposed sociopolitical norms or punishable under the Computer Crimes Law[178], but not with respect to the use of circumvention tools per se.[179] This official posture, in conjunction with the relative comfort provided by the users' knowledge that "everyone does it", has lead to a situation where "anti-filtering tools are used as if they were in fact legally permissible."[180] As Abadpour and Anderson conclude in their qualitative study, "these users may not see bypassing such systems as an act that contravenes political or social structures any more than running a red light at an empty intersection."[181] On-the-ground dynamics suggest that circumvention tools, and the use thereof, are not considered as anomalous behavior, but are rather inherent to the daily habits of the general public. In turn, this naturalness in dealing with the issue of circumvention should be taken into consideration when thinking about the design, properties and implementation details of a tool that is supposed to resonate with Iranian users. The contrary assumption (circumvention is considered as deviant behavior) might place constraints on development efforts that do not necessarily reflect user needs and attitudes on the ground, and could come at the expense of other useful tool properties. Tool developers' concerns in this regard figure for example in deliberations on the "traceability" of tool usage, or whether - due to security concerns - it would deter users to make use of a tool if it had to be downloaded or installed on a device.[182] This suggests an environment where the act of circumvention itself is an exceptional phenomenon which requires the user to conceal the act at all costs.[183]

[176] / *Iran Media Program/ASL19 (2013) - "Internet Censorship and the Fog of Fatwas"* Fatwas are moral decrees issued by high ranking religious authorities, supplementing formal laws.

[177] / There are occasional public statements by government representatives and security forces declaring that the use of circumvention tools is illegal. However an explicit legal prohibition does not exist,, and these public statements have been described as campaigns of intimidation. See footnote 22.

[178] / *Article 19 (2013) - "Computer Crimes in Iran: Online Repression in Practice"*

[179] / During our research and expert interviews, we did not come across any publicly documented cases where the use of circumvention tools served as the reason for legal prosecution.

[180] / *Iran Media Program/ASL19 (2013) - "Internet Censorship and the Fog of Fatwas"*

[181] / *Anderson, Abadpour (2012) – "Fights, Adapts, Accepts: Archetypes of Iranian Internet Use"*

[182] / See for example a discussion on the reasoning behind the design of the first generation of Psiphon, a private web-based proxy. The system would only allow access to those users in censored countries who had a trusted individual in an uncensored country who was willing to run the proxy application for them. The censored user would not have to install any software. One of the reasons for this decision was to avoid traces on the users‘ computer. *Ethan Zuckerman(2007) - "Ron Deibert on the history and future of Psiphon"*

[183] / This scenario would also apply to high-risk, sensitive communication which would also require a tool that provides strong anonymity and privacy.

In relating back to the above noted “tacit agreement” between Iranian authorities and the audience of circumventing users, one can draw the line to some of the common problems encountered by users when using circumvention tools. Instead of prosecuting the act of circumvention, authorities resort to other demonstrations of force. Government interferences in the network have been a regular occurrence in the post-2009 election Iran. Disruptions in the form of blocking or throttling of specific ports and protocols used by circumvention tools have repeatedly hampered their utility. These disruptions, however, have for the most part been limited in scope and efficiency, as the multiplicity of available tools and the sophistication of a certain range of available circumvention systems afforded Iranian users loopholes that allowed them to shift to working solutions and stay connected in the face of disruptions.[184] In this respect, the course of events in the run-up to the June 2013 presidential election is alarming, as it suggests a significant alteration of the dynamic. During the first stage of the multilayered blocking campaign, in early March, the Iranian government blocked VPN ports, depriving users of the most popular category of circumvention tools in Iran.[185] Government vetted “legal VPNs” were proposed, aiming to segment circumvention related VPN use from VPN traffic related to the needs of businesses and other relevant official institutions - an endeavor which, for now, has been abandoned due  to a lack of feedback. During the second stage of the blocking campaign, the government escalated its crackdown on circumvention tools by implementing Deep Packet Inspection (DPI), fingerprinting and disrupting unknown and random traffic, accompanied by heavy throttling of protocols essential to the use of circumvention tools and other encrypted applications and services. As researchers have pointed out, through this wholesale confrontation, the government imposed a “whitelist” system on connectivity, effectively rendering nearly all available circumvention systems useless: “The new filtering rule fundamentally broke the strategy that circumvention tools have thus far implemented to avoid filtering through DPI, wherein they sought to avoid creating a detectable traffic pattern. Iran effectively approached a “whitelist” of permissible applications with a three tier structure for the handing of Internet traffic that traverses the international gateway.”[186] Those few tools that withstood these measures were severely constrained in their utility due to heavy throttling. Researcher Collin Anderson notes: “These technical impediments were creative in a manner that few developers or researchers appeared to have ever predicted.”[187] In relating back to the Iranian tool user, it appears evident that user experience and utility of circumvention tools will, now more than ever, be determined by the tools capacity to stay functional and keep users connected in the face of the Iranian governments’ significant advances in blocking - and their readiness to bring international traffic to a halt if necessary.

The issue of blocking resistance can be expanded to another problematic pertaining to Iran’s circumvention tool ecosystem. As instances of blocking narrow the range of functional tools available, the majority of Iranian users acts from necessity and is compelled to turn to unknown, less reputable and, eventually, unsafe solutions. The detrimental side effect of this dynamic is further amplified by the omnipresent hazard of malware which complements filtering and blocking as an additional mechanism of inter-

[184] / Iranian users report the tools they have shifted to after the government had disrupted traffic to Tor: *Twitter*

[185] / *Reuters (2013) - “Iran blocks use of tool to get around Internet filter”*

[186] / *Small Media (2013) - “Iranian Internet Infrastructure and Policy Report (April-June) “*

[187] / Ibid.

ference.[188] In this environment, security vulnerabilities are to a certain extent inherent to the overall procedure of circumvention, from the sourcing of the tool to its usage. Documented cases where malicious copies of Psiphon and Simurgh-e Sabz were distributed to users exemplify the vulnerabilities of Iran's circumvention ecosystem, where, as pointed out by monitoring organizations, the increasing demand for tools "has not been matched by due diligence on the tools being used or the manner that people are obtaining them. In our examples of recent attacks, malware was being distributed through a Google Group claiming to help users by distributing circumvention tools. (...) Several of the services and tools shared online appear to have little assurance of privacy of communications, including one service that was found to have its traffic logs, tagged to usernames, publicly available." [189] These hazards feed into the local discourse surrounding the issue of online monitoring and surveillance, and impact user perceptions and attitudes. Whether through back-door copies of circumvention tools or through "honeypot" VPNs set up by the government or through active hacking - there seems to be a pronounced appreciation among users of the possibility of being monitored by the government or affiliated entities. [190] Consequently, users' relationship to circumvention is ambiguous and marked by implicit suspicion, which also explains the great number of respondents to the IMP survey who reported they would feel insecure when using circumvention tools.[191] It is important to point out that this feeling of insecurity may also stem from uncertainties and a lack of understanding pertaining to the intransparent nature of the technology itself. One of our interviewees, a close observer of Iran's online and social media environment, stated that "there are a lot of users who don't know what it actually is they are doing [when using a tool], it's not clear to them what it really does. They get it from a friend and hope it will be alright. You have people who think it protects their identity and others are just happy to get to Facebook."[192] Interestingly, in Abadpour and Anderson's study, only a minority of user profiles - those who were involved in more sensitive online activities - reported that they would respond to the potentiality of monitoring by taking countermeasures such as heightened precaution in the sourcing of a tool or by using privacy-preserving tools. The majority of users, however, seem to resolve this tension by practicing self-censorship, or by assuming that their circumvention use - even when monitored - will not attract government attention due to the mundane nature of their activities.[193] A glance at Iranian social media profiles abundantly staffed with real names and pictures further indicates many Iranians' priority of access over privacy of communications. For these users, security and anonymity do not seem to be decisive factors when choosing a tool. Factors that are decisive in this respect evolve when taking note of how Iranians envision "a better Internet". When probed into this issue in both a qualitative manner as well as through online polling, "filtering", "reli-

[188] / *Small Media (2013) - "Iranian Internet Infrastructure and Policy Report (Feb.-March) "*

[189] / Ibid.

[190] / *Anderson, Abadpour (2012) – "Fights, Adapts, Accepts: Archetypes of Iranian Internet Use"*

[191] / 46% of the general survey and 41% of the youth-survey reported they would feel insecure or very insecure. *Iran Media Program (2012) - "Finding a Way- How Iranians reach for news and information"*

[192] / Interview, Dec. 20th, 2013

[193] / *Anderson, Abadpour (2012) – "Fights, Adapts, Accepts: Archetypes of Iranian Internet Use"*

ability," and "speed" were of highest concern and figured most prominently as issues that are in need of improvement.[194] Given the determinative role of circumvention tools in Iranian users' Internet experience, this finding is tantamount to demands and expectations Iranian users place on circumvention tools.  As Abadpour and Anderson point out, "in addition to wanting the filtering regime to end, respondents went on to note the need for better anti-filtering tools as a way of improving Iran's Internet."[195] This tendency is consistent with the assessment of our discussion partners who described that, when users have the luxury of choosing between several functioning tools, they seem to base their choice on speed and reliability. The online editor of a foreign based Farsi language media organization, which provides circumvention tools to Iranian users, sums up his experience: "We get tons of emails from people asking us for the tool, or when they experience problems with it. But so far no one has asked about security or privacy issues."[196] The issue of "reliability" most likely translates into the users' experience with the performance and responsiveness of the tool (developers) during past disruption and blocking events. Lastly, it is important to acknowledge social and cultural conditions when investigating the factors that drive Iranian users towards a certain circumvention tool. As the IMP survey clearly indicates, there is a strongly marked reliance on "strong ties" and "weak ties" as sources of information and news - both among the general population as well as the youth.[197] Word-of-mouth recommendation and social networks of trust are therefore prime avenues through which Iranian users learn about new or working tools, troubleshoot existing problems, and disseminate information into the wider circumvention ecosystem, allowing tools to spread rapidly in a viral distribution mode.[198] In an interview with a team member of a tool provider who maintains a large user base in Iran, it was mentioned that "word-of-mouth has been hugely important for us, unofficial communication. This means that you have people e-mailing the tool, literally distributing the tool on USB drives or mentioning it on social media."[199]  Just as much as international media and concerted promotion efforts from the outside are important in order to introduce a tool to core populations of internationally oriented, highly connected and influential multipliers, so is the interplay of strong and weak ties - virtual or not - defining for a tools' popular adoption. The above mentioned blocking campaign against circumvention tools in the run-up to the 2013 presidential election bear witness to this dynamic. After the blocking of VPNs in early March, users quickly shifted to functional solutions like VPN Gate and Psiphon in large numbers. Within a matter of five weeks, Psiphon3 saw an increase in the number of daily unique users from Iran from a little over 100.000 on March 1st to more than 400.00 on April 7th.[200] Remarks from an interviewee who left Iran in 2010 may add contextual depth to these numbers: "In the street where I lived, I set up VPNs for several people, neighbors, and acquaintances. When something didn't work and we

[194] / Anderson and Abadpour ask how a better Internet would look like, both in the 2012 qualitative study as well as through online polling conducted by Arash Abadpour in 2013. See *Arash Abadpour (2013) - "An Open Letter to the Future President of Iran"*

[195] / *Anderson, Abadpour (2012, p. 20) – "Fights, Adapts, Accepts: Archetypes of Iranian Internet Use"*

[196] / Berlin Workshop, August 8-10, 2013

[197] / The online youth-survey ranks strong ties as the third most important information source (49%), just as general survey (51%).

[198] / This modus operandi certainly has a flip side, as it allows malicious tools to spread similarly.

[199] / Interview, August 30th, 2013

[200] / *ASL19 (2013) - "Psiphon3 Data and Graphs"*

met each other outside, they asked if I could come by sometime and take a look. For some of them I had installed several pieces of software. At least one or two were always disrupted."[201]

## Toward Expanding Usage and Utility of Circumvention Tools

In light of the various limitations related to the status quo of circumvention tool development and usage, as well as the above described difficulties emanating from the situation, we hereby suggest all actors with the capacity to implement or help implement policy changes to consider the following recommendations:

Adapt circumvention systems to the peculiarities of Iran's network environment. Iran's Internet infrastructure is heavily compromised and network outages and disruptions - whether deliberately imposed or as an unintended byproduct of its security oriented governance - are an everyday occurrence. Iran's international connectivity is regarded as one of the most unstable in the world.[202] Heavy throttling of specific protocols and potentially all outbound traffic has been attested through measurements[203] and confirmed by Iranian officials. [204] In May 2013, the median connection speed was slower than a dialup modem.[205] Furthermore, the unprecedented blocking campaign in the run-up to the 2013 presidential election demonstrated a degree of sophistication that overwhelmed the capacities of most circumvention systems available to the average Iranian user. These developments are concerning, particularly in light of the expanded fiscal support for tool development and the multiplicity of tools that have been deployed.

To a large segment of Iran's Internet users, the utility of the Internet itself is inextricably linked with the performance of the available circumvention tools. To the extent that providers want to focus on circumvention systems for Iranian users, they should evaluate the tool s' properties and implementation details in due consideration of the features of Iran's network environment and the government's advances in blocking techniques. This can mean ensuring low latency in order not to augment the effects of throttling, allowing users to opt-out of proxying traffic to domestic websites or pre-caching sites that Iranian users often visit. The blocking events surrounding the elections strikingly demonstrated the significance of blocking resistance as a core necessity for Iran focused tools. In terms of tool architecture, Psiphon3's multiprotocol design has turned out to be an effective precautionary measure. As the Iranian government blocked VPNs in early March 2013, Psiphon managed to stay functional by connecting users through its obfuscated SSH protocol which resisted the subsequent implementation of deep packet inspection. Aside from properties that are related to the basic architecture of the tool, or more sophisticated ways of avoiding detectable traffic patterns in order to reduce the tool's vulnerability to targeted disruptions, tool providers could take measures to increase the response capacity to blocking attempts. The ability to respond in an effective and timely manner is usually constrained by a lack of information on the nature of the blocking event, the applied mechanisms, and the impact on user experience. Tool providers who choose to focus on Iran will inevitably experience

[201] / Interview, October 8th, 2013

[202] / *Small Media (January 2013) - "Iranian Internet Infrastructure and Policy Report"*

[203] / *Collin Anderson (2013) - "Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran"*

[204] / *RFE/RL (2013) - "Iran Admits Throttling Internet To 'Preserve Calm' During Election"*

[205] / *Small Media (2013) - "Iranian Internet Infrastructure and Policy Report (April- June)"*

performance disruptions and blocking attempts on a regular basis, and Iran is known to adjust their censorship mechanisms frequently. Viable mechanisms which allow the user to provide information with as little effort as possible should therefore be incorporated in the provider's strategy or tool design, as they can be a direct contribution to the blocking resistance of a tool.

In the case of Psiphon3, a built-in feedback button allowed users to submit encrypted diagnostic data, which reportedly resulted in user feedback at the rate of thousands of messages per day during the blocking campaign prior to the elections.[206] As laid out in ASL19's detailed analysis of the political and technical developments, the team's access to users and feedback diagnostics were decisive in ensuring the tools' availability throughout the entire blocking campaign.[207] Seven updates could be released within five weeks, whereby sustained feedback loops contributed to the continuous refinement of releases that were deployed. Circumvention systems that rely on client-side applications release different versions and updates, and keeping track of these updates can be both critical and burdening for users, especially when the effects of interferences and blocking turn out to be as severe as in the case of Iran. By avoiding the necessity of manual intervention by the user, Psiphon was reportedly able to deliver the critical fixes to 90 percent of its user base by the time of the election through the auto-update feature of the tool. To ensure that updates would be received in spite of recurring disconnections due to deep packet inspection, users were able to resume downloads when connections were dropped. Features like build-in feedback mechanisms, automatic updates, and resumable downloads might be auxiliary benefits when compared to more sophisticated contributions to blocking resistance like traffic obfuscation, however, in highly contested network environments like Iran's, these auxiliary properties can add up and tip the balance against state imposed blackouts like users have experienced in Iran.

Lastly, Feedback mechanisms as implemented by Psiphon are only helpful insofar as the team's resources allow them to act thereon and respond to the influx of information. In this context it is worth mentioning that, in most cases, response-driven development and deployment can rarely be executed fast enough to make a difference, as a lot of circumvention projects are maintained by dedicated, but small and poorly-resourced teams. For Iran focused circumvention projects, it is therefore all the more important to appreciate broader patterns in Iran's Internet control policies, as they suggest a strong correlation between sociopolitical events of significance and interferences in the network.[208] Contextual awareness allows developers to arrange for rapid response capacities in order to preempt and mitigate foreseeable disruptions.

Build networks of trust and contextual knowledge to expand adoption of Internet freedom tools. In most cases, Western developers provide circumvention tools that are supposed to resonate globally. Patterns of adoption and utilization, however, are shaped by social and political conditions and can vary significantly between countries and regions.  From the providers of tools, this demands different approaches and levels of effort. The majority of Iranian users base their choice of tools and methods on recommendations from sources they trust[209]: friends, family, acquaintances, and diaspora networks provide infor-

[206] / *Psiphon Team Blog (2013) - "Psiphon and the 2013 Iranian Election"*

[207] / *ASL19 (2013) - "Information Controls: Iran's Presidential Election"*

[208] / Ibid.

[209] / The differences in adoption patterns are illustrated in a recent survey on tool usage among Chinese users. Personal recommendations were of little importance to the surveyed Chinese users. See *Open ITP (2013) - "Collateral Freedom"*

mation on tools as well the tools themselves, and online social networks have expanded the network of trust to include virtual connections. These trust based modes of education and sourcing of tools have on the other hand been severely burdened and disrupted by the circulation of malware and malicious tools, intimidation by the state, as well as the widespread conviction of being monitored while being online. This has created an atmosphere of anxiety and suspicion towards online platforms and activities in general, and towards the issue of circumvention in particular. All of our discussion partners who closely interact with Iranian users on online platforms and provide or educate users on circumvention tools and digital security have described the clearly noticeable increase in suspicion and mistrust within user communities. From outside circumvention tool projects that aim to resonate in Iran's circumvention ecosystem, these adverse conditions might eventually require more than just the provision of technology. In audits and reviews of popular circumvention tools, this problematic is occasionally addressed under the theme of "community support".[210] In practice, more often than not, community support receives only limited attention and resources from tool providers. However, just as much as trust-based adoption patterns distinctive of Iran's circumvention ecosystem can turn out to be an effective barrier to more widespread circulation and adoption of a tool, they can also provide an opportunity. The close collaboration between Psiphon and ASL19[211] does deserve mention in this regard. Consisting of practitioners and researcher of Iranian descent, ASL19 acts as an amplifier in both directions by providing a granular level of country specific information on real-world usage to the developers, as well as localized, culturally nuanced Farsi language support to end-users on the ground. Given the compromised and contested nature of Iran's Internet environment, a suchlike mechanism enables the dispelling of fears and suspicion among users. As a result, a cycle of trust is being generated amongst a critical mass of early adopters and influencers who will consequently recommend and encourage the use of a tool within their communities.

On the other hand, a high degree of responsiveness and networks of trust are necessary in order to maintain an audience inside Iran after the initial uptake of a tool: since disruptions and rapidly evolving digital threats are a regular occurrence, a neglect of trust-building measures and responsiveness can quickly lead to a compromised reputation and a decline in the number of users. The significance of such a network of trust may have become particularly elucidated by a recent example: After the University of Isfahan relayed a widespread news item alleging that the Psiphon tool was extracting private user files from mobile phones and computers, cooperation with users enabled enhanced responsiveness on the part of Psiphon and ASL19. Thus Psiphon's ability to quickly respond to allegations and to react to users' concerns prevented a decline in trust and user numbers. An effective strategy for Iran therefore requires increased investments in outreach and communication. Circumvention tool providers may therefore be well advised to incubate and partner with communities of country-experts who can provide localized peer-to-peer support in order to leverage the trust-based adoption patterns on the ground.

Address unmet demand for mobile circumvention. There were few circumvention related topics where the assessments of our discussion partners were as definitive as with respect to the significance and potential of mobile circumvention for Iranian users. One interviewee's remark sums up this consensus: "This is probably the biggest gap. If you look, there is so much demand for all kinds of devices and

[210] / *Freedom House (2011) - "Leaping Over the Firewall - A Review of Censorship Circumvention Tools"; Berkman Center for Internet & Society (2009) - "2007 Circumvention Landscape Report: Methods, Uses, and Tools"*

[211] / *ASL19*

there is only little choice. And if they close VPNs again, there is pretty much nothing left." There is a strong and unmet demand for circumvention systems on range of portable devices in Iran, which is facilitated by several indicators. Mobile phone penetration has grown from 41,7 percent in 2007 to 76,9 percent in 2012, and despite tight government control over licensing of mobile operators, 17 cities are under partial 3G coverage.[212] The use of mobile applications has become a daily routine of Iran's youthful population, which figures in numbers released in mid-2013: 4 million users of the Android operating system have reportedly accounted for 10 % of the entire web traffic of the country, and Cafe Bazaar, a localized version of the Google Play application store, alone has generated 2% of the traffic.[213] As aforementioned, Iranian users have been particularly swift in adopting a range of messaging and VoIP applications like WhatsApp, Viber and WeChat, which have been spreading like an avalanche among the mobile equipped population. The prominent role these applications have come to play as an essential enabler of popular communications culture was mirrored in an intervention by Iran's Supreme Leader Ali Khamenei himself, who declared online messaging applications as immoral via religious edict in January 2014.[214] These applications have been blocked one after another, which has done nothing more than fuel an already widespread demand for mobile circumvention systems. Data shared by Psiphon indicates that of the 800.000 daily unique users of the Psiphon 3 application[215], one third connect to the network using the mobile Android version. These numbers illustrate the status quo before the Iranian government blocked the popular social messaging application WeChat in December 2013. Within 4 days after the blocking, Psiphon reported a surge in activity on the network, caused by 600.000 new users of the tools' mobile Android version. These dynamics indicate the significance of mobile solutions in Iran's circumvention ecosystem. Similarly, they shed light on the potentials and significant amount of users who are still unaddressed. For now, the majority of Iranian users whose devices, operating systems and software versions are not supported by developers are still on the sidelines. The current supply of purpose-built circumvention tools covers only a fraction of the existing demand, as most of the available systems do not support portable devices in the first place. Circumvention tool projects that succeed in allowing those on the sidelines to circumvent censorship on their mobile devices will in turn have a significant advantage in terms of popular and widespread adoption inside Iran. Furthermore, the availability of mobile circumvention solutions might - due to the ubiquity of mobile devices - eventually help in introducing the issue and benefits of censorship circumvention to segments of Iranian society who have so far been unaware of the existing options.

Explore and utilize opportunities for "interventions" to increase awareness and security. Although Iranian users are skilled in evading censorship, this savvy is seldom matched by an understanding of the implications that are attached to the different methods and tools for circumvention. Iranian users usually have to experiment with several methods and tools until they succeed in connecting to the network, and it is hardly possible to familiarize oneself with the multiplicity of tools that circulate. Language barriers furthermore add to the confusion and security risks. While making use of circumvention tools, the feelings of insecurity as described above are therefore directly linked to a lack of awareness and conceptual understanding, both of which might have security implications.

[212] / *Freedom House (2103) - "Freedom on the Net"*

[213] / *Small Media (2013) - "Iranian Internet Infrastructure and Policy Report (June-July)"*

[214] / *Al Arabiya (2014) - "Iran's Khamenei bans online chatting between unrelated men and women"*

[215] / *ASL19 (2013) - "Psiphon3 Data and Graphs"*

On the part of the developers of circumvention tools, efforts to address these interrelated issues usually pertain to rather technical audits of the security and integrity of the software. In most cases, providers refer to additional manuals and documentation in order to help the non-technical end-user to comprehend the application of the tool, the security it provides, and the risks users take in employing the tool. Efforts to support the user in this complex process point almost exclusively to the demand side: after having obtained and installed the software, the user is expected to browse to the providers' or third party websites, source the manuals, and work through the documentation. Once contrasted with real-world usage as described so far, this scenario does not match the average Iranian users' capacity and disposition. The struggle that is involved in establishing an unfettered connection marginalizes concerns about security implications, and the sourcing of a tool is seldom followed up by efforts to acquire further information.

Similarly, developers and third party providers tend to address and promote circumvention separately from the task of awareness raising and education. In most cases, the latter two are addressed in the framework digital security and hygiene. Developers and organizations which distribute circumvention tools to Iranian users should rather try to actively connect both realms. From the downloading of a tool to its application by the user, the path of circumvention provides multiple opportunities for small "interventions" that should be explored and utilized in order to inform the user, raise basic awareness and security.
Developers and third party providers should explore the opportunities they have to "intervene" and proactively guide the user towards relevant resources and enable more informed decisions with regard to circumvention. For example, a range of circumvention tool providers have set up e-mail auto-responders, through which users can request their tools, while other providers also push their tools in mass email campaigns. These measures of tool distribution could also serve as an opportunity to provide lightweight resources that convey basic understanding of the regularities of censorship and circumvention, inform the user on the range and differences of methods of circumvention, and allow the user to eventually spread this knowledge by forwarding the tool to friends and colleagues.

On the other side of the spectrum, developers could make much more pronounced use of opportunities provided by the tool during the process of its application, by using design and the multiple layers of the tool to make visible and transparent the nature of the product, what is happening at every step of the process, and the promises the tool is making with regard to confidentiality and security. Communicating these properties through adequate design can mitigate the risks and chilling effects that shape the circumvention experience of a non-technical, non-English speaking user who deploys a tool in a compromised Internet environment. Similarly, the range of third party providers who promote tools and resources to Iranian users should realistically evaluate in how far the finer arrangement and configuration of their platforms is suitable to guide a user, whose primary concern is a functioning tool, to information resources that are relevant in the context of circumvention. This requires a thought out placement of links and arrangement of navigation items in order to grab the users' attention and actively steer the user towards relevant resources before the tool is deployed.
These opportunities for small "interventions" cannot replace broader efforts of digital security education. However, they could increase the margin of security and awareness by leveraging the outstanding importance of circumvention to users in repressive online environments.

Enhanced privacy features should not limit rich media usage and speed. One of the defining challenges with regard to the development of circumvention systems is to find the balance between tool properties that allow for a reliable connection to today's web 2.0 multimedia content and properties that ensure robust privacy and anonymity. Embracing one usually comes at the expense of the other. Tools that provide enhanced privacy and anonymity slow the already throttled network and usually disable browser settings that are necessary for multimedia content. Since the benefits provided by circumvention tools are particularly crucial to users in repressive environments, much focus has been put on users who are dependent on the latter category of tools in order to safely carry out their work. To the extent that our previous characterization on user behaviors and needs is indicative of the "average" Iranian user and the most common use cases, this focus might not serve the needs of the majority of Iranian circumvention tool users. These users seem to be willing to trade fast and multimedia enabling tools for privacy and anonymity preserving ones. Circumvention is of utter utility because it enables them to access mundane information relevant to their daily routine, to establish and maintain relations through Instant Messaging, email and on social media platforms, and to keep pace with global online trends that provide dynamic and rich media content. These users handle the lack of privacy and anonymity either by adapting their activities to the potentiality of being monitored, or by ignoring it because their activities are not expressly political. To these users, an encrypted connection to a server outside the government's reach might fulfill their privacy needs, since the government and its affiliated entities are considered as the prime adversary, whereas enhanced anonymity features will most likely be experienced as limiting. The majority of Iranian users do not shy away from tools that have to be installed[216], and they habitually have a range of tools at their disposal. These traits are in part the side effects of an online environment, where users have to be flexible in order to stay connected and cannot afford to rely only on their preferred type of tool. The circumvention tech community could meet the needs and facilitate the unfettered online activities of a large audience by providing tools whose privacy and security properties do not constrain these user needs.

[216] / VPNs are the most popular generic category of tools among Iranians, despite the fact that they have to be installed and configured, which demands a relatively higher level of effort from the user.

(Disclaimer: This chapter will emphasize the outcomes and problematic of sanctions, mainly from a US perspective, to the detriment of other countries with similar legislation. This perspective has been selected as most of the services relevant to the Iranian communications environment are based in the US, and therefore subject to its legislation. Similarly, the US constitutes a particularly politically influential factor and driving force in policy-making.)

### Discussion

Sanctions continue to be a main determinant in the relations between Iran and the rest of the world, and no discussion on Iranian digital communications could be conducted without investigating the impact of this set of legislation. The basis for such a discussion of sanctions directly relating to Iranian digital communications dates back almost 20 years[217], when William Clinton announced a comprehensive ban on US trade and investment in Iran. These sanctions, whose most recent renewal had been announced under the first Obama administration in 2010[218], are supported by similar legislations of the EU[219], Canada[220], Australia (announced)[221], and Japan, and are continuously barring the delivery of technology, software, and hardware into Iran.

For years sanctions in this way have prevented the delivery of both software and hardware, and in the case of the US, have charged the Office Foreign Assets Control (OFAC), the export control mechanism of the US Treasury Department, with punishing violations with severe penalties ranging from fiscal measures to prison sentences of up to 20 years for natural persons. The prevention of technology deliveries to Iran is thereby achieved through a combination of direct trade sanctions as well as financial sanctions. This not only impedes direct banking relations between the US and Iran, but ever since the injunctions were reinforced after the election of President Ahmadinejad in 2005[222], in their political aftermath the sanctions have also increasingly ended relations between European and Iranian banks.[223] Since January 2012, Washington has furthermore sanctioned Bank Tejarat, Iran's third largest bank, under a U.S. executive order aimed at "targeting people and companies that promote the proliferation of weapons of mass destruction as well as their support networks". In effect this bank and every bank engaged in business with Bank Tejarat, were thus cut off from the US financial system. Despite the US having previously undertaken such an effort, Bank Tejarat's case is particularly remarkable because it had been the last major Iranian bank available for legal trade in Iran. From now on, companies need to channel transaction through significantly smaller banks, thus rendering their business even more time-, cost-, and organization- intensive. Moreover, in a latest move, since June 2013, the US government has authorized sanctions on any foreign financial institutions conducting "signifi-

[217] / In 1995 President William Clinton announced a comprehensive ban on U.S. trade and investment in Iran, a move codified by Executive Order 12959, see for example *Council on Foreign Relations (2013) - "The lengthening List of Iran Sanctions*

[218] / *US Department of State (2011) - "Fact Sheet: Comprehensive Iran Sanctions, Accountability, and Divestment Act (CISADA)"*

[219] / Regulations 1263/2012 and 1264/2012

[220] / *Foreign Affairs, Trade and Development Canada (2013) – "Iran: New Developments"*

[221] / *Australian Government (2011) - "Public Consultation on Australia's sanctions relating to Iran"*

[222] / Congress passed a bill in 2006 strengthening the August 1996 Iran Sanctions Act (ISA)

[223] / This is highlighted by the latest conclusive move by Europeans to disconnect Iran from the European based clearinghouse system for financial transactions SWIFT.

cant transactions" in the Iranian rial.[224] In spite of such a comprehensive regime of regulations, sanctions have, although leading to a situation where notorious "dual use" digital repression tools can no longer be legally imported into Iran, not been able to prevent hardware and software products of Western origin entering the country via black-market trade[225]. Critical downloads for software and updates such as instant messaging, anti-virus, Java, Flash and similar services had meanwhile become effectively disrupted, leaving Iranian Internet users prone to security and access vulnerabilities.

A common lobbying effort has thus been initiated by a coalition of NGOs and advocacy groups such as ASL 19, Access Now, International Campaign for Human Rights in Iran, or the National Iranian American Council, to persuade both US government officials, as well as corporate actors, to change those aspects of the sanctions regime that were detrimental to Iranians' pursuit of free speech and contradictory to the State Department's Internet Freedom agenda.

An initial success of these efforts had been the issuing of exemptions on software for personal communications from the sanctions by OFAC on March 8, 2010, a modification which nonetheless two years later proved of insufficient efficacy to the policies of corporations. As a result the same civil society actors found themselves compelled to address corporate actors in an open letter to implement the exceptions.[226] Continuing pressure of this coalition led the US Treasury and OFAC to exempt all personal technologies in May 2013 with the issuing of General License D.[227] Under this license US persons can legally export electronic and communications equipment including cell phones, modems, laptops, tablets, antivirus software, anti-censorship tools, and Virtual Private Networks. The license even allows for the financial transactions incidental to these exemptions which must nonetheless be effectuated through intermediary third country banks.[228]

Sanctions on communications devices remain intimately tied up with a set of difficulties which are the direct results of such regulation. In general, a two-fold problematic appears to emerge from the legislation pertaining to problems arising from the formulation of the legislation and the very structure of the sanctions, exceptions, as well as architectures of implementation. An expert has thus recently concluded that: "in spite of the general license, there has been no real feedback, no major opening of services."[229] The following case study shall exemplify this problematic:

224 / *NYTimes (2013) - "US adds to its list of sanctions against Iran"*

1263/2012 of the EU prohibits EU financial and credit institutions transferring funds to or from Iranian financial and credit institutions, without prior authorization. See for example *Holman Fenwick Willan (2013) - "Iran Sanctions Update: the EU implements new restrictive measures"*

225 / *Citizen Lab(2013) - "Planet Blue Coat"*

226 / *NIA (2011) - "Internet Freedom Letter to Tech Companies"*

227 / *Department of the Treasury (2013) - "OFAC-General License D"*

On 9-11-2013 OFAC additionally issued another two licenses D and F. The first general license, General License E, authorizes the exportation of services and funds transfers by nongovernmental organizations in support of certain not-for-profit humanitarian activities designed to benefit the people of Iran. General License F authorizes the importation and exportation of certain services in support of professional and amateur sporting activities and exchanges involving the United States and Iran.

228 / "However, U.S. depository institutions are permitted to handle funds transfers, through intermediary third-country banks, to or from Iran or for the direct or indirect benefit of the Government of Iran or a person in Iran, arising from several types of underlying transactions, including: e) a transaction authorized by OFAC through a specific or general license."

229 / TFI Workshop, August 8-10 2013. More recently however, little progress has been achieved, most notably by the companies Google and Apple

During August 2013 the website www.karroubi.ir of Mehdi Karroubi, a leading Iranian opposition figure, had been shut down by a US web hosting company, citing the ongoing sanctions imposed by OFAC.[230] Investigating the issue, Collin Anderson, a researcher affiliated with the University of Pennsylvania, provides some valuable insight on the short-comings of the general license which still leads to unfavorable interventions[231] and side effects in the Iranian policy environment. In order to understand the issue, according to Anderson, it is useful to assume the position of the corporate lawyer facing the decision-making process: Not only would such a lawyer be confronted with a legislation that does not explicitly exempt web-hosting, he would also, especially assuming that the lawyer is a non-Farsi speaker, have had trouble identifying whether the person in question was affiliated with the Iranian government or using the website for personal communication. A non-Farsi speaker would furthermore run the risk of picking a wrong transliteration (the process is not standardized) in the tedious task of cross-checking the website owner with the list of Specially Designated Nationals providing the exceptions to the exemption. He would consequently have had to make a decision against the background of exemplary cases where substantial penalties had been imposed on corporations violating the sanctions for a benefit of a hosting fee of as little as USD 5.- a month.

This example may be particular, yet it not only highlights the remaining formal issues of a legislation which could be formulated in a more inclusive fashion, but also all of the structural factors that illustrate the prevalence of corporate over-compliance and the slow pace of improvements inside Iran. As the example amply indicates, a simple cost benefit calculation taking into account the complicated and time consuming vetting process as well as the substantial financial risk through ambiguous wording already tip the balance in favor of acting conservatively and risk aversely with regards to transactions. Ever since the shutdown of Bank Tejarat for international trade, companies have had furthermore difficulties of obtaining payment for their services.[232] One must also take into account the complicated process of funneling transactions via third party banks, of which it is not certain whether their risk assessment is not even more conservative, to small Iranian banks. Previously, in a situation where even the shipping of medical goods has caused substantial problems, it is not sure why communications devices should cause less of a nuisance.

Moreover, from a political perspective, an OFAC, whose very raison d'être consists in the enforcing of sanctions, risks substantial political pressure for being soft on the implementation of sanctions, adding the risk of legal ambiguities being interpreted in a restrictively leaning fashion, in order to pay tribute to those political forces eager to see US-Iranian relations reduced to a minimum.

## Toward Improving the Sanctions Problematic

In light of the various shortcomings related to the status quo of sanctions policies, as well as the above described difficulties emanating from the situation, we hereby suggest all actors with the capacity to implement or help implement policy changes to consider the following recommendations:

[230] / *VOA (2013) - "US Company Shuts Down Iran Opposition Website"*

[231] / Through blocking of a moderate politician in opposition to the former government.

[232] / Reuters (2012) - "Exclusive: Of diapers and drugs, Iran's trouble paying bills"

Clarify the legal base of sanctions. This recommendation ultimately refers to extending the existing provisions to become more inclusive and less ambiguous. It also aims at finding ways to avoid facilitating heavily bureaucratic processes and generating security for those aimed at providing communications hard- and software for Iranians. Creating advisories- contact points with trained legal staff in order to facilitate the modification of legislation could be an important step in order to generate security. Such advisories could similarly, in the absence of legal modifications, help corporations with legal assistance, since one problem as noted by a TFI workshop participant was the lack of specialization of corporate lawyers which would often conduct them to not take a risk. Clarification could also be undertaken by the respective sections of the US government, particularly the Department of Treasury, the Department of Commerce, and the Department of State, all of which can ensure informational outreach and improved clarity about the licensing process to commercial actors. A call to clarification or legal assistance seems all the more urgent, since the unambiguous political decision which acknowledges the benefit of personal communications technologies for Iranians has already been taken, and ought therefore not to be paralyzed by organizational circumstance.

Continue comprehensive lobbying, adding on to the past successes to generate public pressure on corporations not implementing licenses which had been granted to them. If the decision making process of commercial actors at present tips the balance in favor of a non-implementation, then the costs of such a decision should be increased. In the past, good experiences have been made by using Internet freedom fora to address the responsible representatives of relevant corporations directly and thereby generating public pressure. Other suggestions by representatives from NGOs include creating a publicly accessible website listing public services which ought to be accessible, to generate a more publicly available mechanism of creating accountability as well as staffing and updating it. Funds are necessary for such an encounter, since it requires a continuous research effort.

Incentivize corporate involvement. The most powerful argument remains in appealing to Iran's potential as a future market, for which both advertisers and tech- corporations are building the cornerstones of a future competition. Market shares in such an environment are still to be gained relatively easily. It can be assumed that a company that can be convinced to become involved in the Iranian market will be followed by its competitor, thereby creating a dynamic which ultimately benefits Iranian civil society. The same civil society as a consequence becomes the object of corporate competition extending the offer of services in order for private actors to obtain market shares. Advocacy organization should therefore focus on the least risk-averse enterprises with the greatest potential gains. Once market access is obtained by these parties, other big corporations are likely to follow suit. Examples of such economic pioneering can be seen in the recent opening of the Google Play store for customers in Iran[233], the announcement of Apple to ship previously restricted hardware into the country[234], as well as the opening of Persian language targeted ads for Google's AdWords service.[235] Especially the latter is setting an important precedent, with online advertising constituting the basis of modern independent media. Therefore, the stated examples may not be

[233] / Washington Post (2013) – *"Why google broughts its app store to Iran and what it could mean for Syria"* The policy applies to date only to free services. The app store had meanwhile been blocked by Iranian authorities.

[234] / *The Verge (2013) - "Apple will begin shipping previously restricted hardware to Iran"*

[235] / *Iranwire (2013) - "The beginning of the End of Digital Prohibition? Google & Apple's Decision to Allow Iranians Digital Access"* Adwords is still only Persian language based and License D is yet to be interpreted in a way to enable it to target Iran.

far-reaching, yet may well constitute the commencement of an interesting dynamic which will create a competitive environment for the Iranian market in the long run, and in the process serve Iranian users by making all services allowed for by the exemptions in the list of sanctions available.

Create designated payment channels. The existence of a rigid financial sanctions regime in place against Iran has a strong detrimental effect on a free communications environment inside Iran. Sanctions hurt Internet freedom by depriving the Iranian public of the beneficial side-effects, so-called ‘collateral freedoms’, of market liberalization and interdependencies which impose heavy costs upon governments aiming to censor content.[236] While the select liberalization of services like Google Play is a welcome step into the right direction, it will not suffice in generating the necessary impact if users are unable to access paid-for services. In order to incentivize commercial actors to provide paid-for services, a lessening of the chilling effects of the sanctions regime could be achieved through the installation of designated payment channels, with trained staff to process non-sanctioned transactions. Such channels are necessary in order to generate legal security for commercial actors seeking to navigate through the complicated requirements for a licensing of transactions. In return such a designated payment channel will generate the necessary safety measures for vanguard financial transactions, which will serve as precedents for a more regular exchange and transfer of personal communications devices and services with the capacity to strongly impact Iranian Internet freedom.

[236] / For example through shared hosting of content enabling users to circumvent censorships on platforms used for services indispensable to the government. For more information see *Open ITP (2013) - “Collateral Freedom”*

« content

### Explanatory Note

Formulating strategies that could serve to counteract limitations on connectivity and freedom of expression imposed through Iran's Internet policies also means closely observing and anticipating its main developments. The range of issues addressed in this report were inspired by the experiences and insights of the multiplicity of our interview partners who have been observing and reacting to Iran's Internet policy developments for a number of years. As indicated by news items as well as individual research efforts[237], the Iranian government's plan to develop a self-contained National Information Network[238], parallel to the global Internet, likely amounts to one of the most significant alterations that the coalition of forces seeking to facilitate information flows will be forced to cope with. Although the issue resurfaced in discussions with several experts, it figured prominently in interviews conducted with Iranian Internet researcher and blogger Arash Abadpour.[239] His viewpoints on the potential implications of the National Information Network for Iran's online dynamics stood out, due to the fact that they went beyond a description of the severe limitations that are to be expected, and reflected on the problematic in a proactive manner, based on the worst-case scenario: the cutting off of connections to the global Internet. By virtue of this approach, the presented viewpoints probed into the National Information Network in search of opportunities and dynamics that could counteract the agenda that the Iranian government is trying to advance with this project. We asked Arash Abadpour to provide a summary of his viewpoints to be included in this report, as they can give new impetus to the public discourse on the National Information Network, and spark debate that could lead to a better preparation of all stakeholders who could contribute to mitigate its disruptive ramifications. Meanwhile, in order to have an informed debate, it could already be claimed that there exists a clear need of research on the technical properties of the network, building up on existing efforts.

## *Arash Abadpour*

### Introduction

There are many indications that the Iranian Internet establishment is going forward with the plans to "nationalize" the Internet in Iran. While, from a technical perspective, the term "National Internet" is an oxymoron and should be avoided, this project is an umbrella attempt to significantly alter the Internet regime in Iran.

It could be argued that the current settings of the Internet in Iran consist of a large user-base for multi-national service-providers such as Google and Facebook. As expected from the track record of the Iranian establishment, the fact that millions of Iranians can communicate on the Internet is not acceptable. The regime uses technical and jurisdictional tools in order to infiltrate online networks, to identify individuals and groups, and to silence them. These efforts have failed during sensitive times, e.g. before, during, and after elections and other sociopolitical developments. One suggestion is that the Iranian regime intends to occupy the Internet, through extending its control from

[237] / *Anderson, Collin (2012) – "The Hidden Internet of Iran"*

[238] / See Part 1, Chapter 1.

[239] / Arash Abadpour holds a Masters of Science in Computer Sciences and a Ph.D.in Electrical and Computer Engineering. He has been a blogger since October 2004, under the pen name Arash Kamangir. His Persian blog *Kamangir* is among the twenty most-read blogs in the Persian blogosphere based on different statistics. Arash Abadpour is regularly consulted and interviewed on developments in Iran's online environment. He provides commentary regarding the Persian blogosphere and has been involved in a number of research projects related to the relationship between Iranian users and the Internet. More information on his research is available under *http://abadpour.com/*.

being the gate-keeper to being the sole provider of the services. In laymen's terms, the National Internet is an attempt to enable cutting the population off from the outside world, and to guarantee that the content which circulates the Internet is stored in machines physically located inside the Iranian borders.

The National Internet project differs from the dominant filtering machinery, in that it provides a positive control mechanism. While the filtering regime causes hurdles and attempts to stop individuals from accessing forbidden content, therefore utilizing negative control mechanisms, the positive approach of the national Internet project is to offer an ocean of content which is safe to consume, from the perspective of the regime. Additionally, in contrast with the filtering regime which limits access to communication methods, such as email, during sensitive times, the national Internet project will guarantee that email and other means of communications happen on heavily monitored networks and originate from and end in monitored servers. In effect, the national Internet project differs from the filtering regime in that it eliminates the alternatives.

The history of the Internet in Iran has many commonalities with the fate of other means of public discourse, i.e. the citizenry is deprived of building social capital unless it is in accordance with the ideology of the system, and dissent is harshly treated. In effect, the public space under the Islamic Republic has had two prominent properties, one, it is heavily controlled, two, the control is widening and deepening as time passes. The key question, however, is whether this trend is expected to be able to continue. In other words, in the context of the imposition of limitations on the Internet, the key question is, whether the possibility exists that the regime is going to become self-defeating.

In the discussion of the handling of the Internet in Iran, one may ponder whether the national Internet project could in fact be the opening of the Pandora's Box for the regime.  It is worth taking a second look at how this undertaking could unfold. The following thoughts are nonetheless not meant to be an endorsement of the national Internet project, but are based upon the assumption that the Iranian government will hardly be swayed in the realization of its vision. While it remains out of the question, that the national Internet constitutes a violation of freedom of expression and access to information, it should nevertheless be considered how and which of the properties of the national Internet could be offering opportunities which could turn out to be challenging to the regime. This contribution provides a summary of some of the possibilities that the national Internet in Iran may provide.

### Let the People Talk

A valid argument is that the national Internet project would allow the regime to disrupt communication between the population of Iran inside the country and the Iranian communities abroad. This communication is obviously important for the Iranian society as it allows for an impression of the possibilities of democracy through the facilities that the World Wide Web offers. For example, an Iranian outside the country can provide anecdotes from her life in a liberal democracy, a human-rights-focused website based outside the country can report on violations, and a documentary on non-violent means for questioning authority can teach the Iranian population. The said communication is also critical for the Iranian "diaspora" in order for it to avoid becoming obsolete and irrelevant.

The national Internet project could cut off the aforementioned communication or, at least, may threaten to disrupt such links. This obviously is a loss for both parties, but, nevertheless, it does not explicitly translate into the parties being forced to stop the conversation. In fact, the national Internet project has to offer incentives in order to bring the population on board. Such provisions may include faster connection speed, better geographic coverage, and,

« content

eventually, a stronger legal framework to protect individual's privacy on the web. These measures could in fact encourage discourse within the population. Facilitation of communication among tens of millions of Iranians based in Iran may in fact be an achievement that would dwarf and counteract the cutting off of connections with the Iranian communities outside the country.

### Some Roads Do not Pass Through Rome

While the national Internet project may compartmentalize the Internet by at least cutting off the connection between the population base inside Iran and the outside communities, the fact of the matter is that the Internet is not the only means of communication between the two groups. Many Iranians frequently travel from the outside to Iran and vice versa, and satellite television is not only widespread, but an integral part of the Iranian societies' information consumption patterns. These and other alternative bridges may in fact allow the Iranian population to keep up with developments abroad, its achievements and deficiencies. This information may then disseminate across the high-speed and high-coverage national Internet.

The question is, under which circumstances people in the provinces and smaller cities and rural areas have a higher chance of being exposed to modern concepts such as human rights and state responsibilities, when Internet is unavailable, unaffordable, slow, filtered, and criminalized, or when it is a household window into the collective mind of tens of millions of other individuals. One may argue that the national Internet may provide the platform for the population to digest and localize concepts that it could receive through other means.

### The Afternoon Tea, not a Shot of Vodka

Use of the Internet in Iran requires skills which are outside the scope of many Internet users anywhere else in the world. One has to have an understanding of Internet protocols and be capable of acquiring, setting up, and utilizing a filtering circumvention tool in order obtain access. In effect, what is a simple routine task of clicking on a link in many parts of the world requires a precisely orchestrated sequence of activities in Iran. Not only the complexity of the procedure discourages many prospective users, but the fact that the act of accessing a forbidden page constitutes several illegal activities taints the action and functions as a selective process.

The author has previously argued that blogging in Iran has similarities with the consumption of alcohol and the use of drugs in the country, both of which are dangerously prominent in the Iranian society.[240] In short, the three activities provide relief from the oppression of the system and require a level of risk-taking. It can be argued that the current limitations imposed on Internet use reduce its popularity within the mainstream of the society and increase the relative size of the risk-taker user-base. Going online in Iran is more similar to having a shot of Vodka than taking a sip of an afternoon tea, as the individual needs to prepare for the activity, gets the buzz of satisfaction for having committed an illegal activity, and is in danger of prosecution.

While one may argue that change in a society may be more associable to fringe elements than the common risk-averse, the possibility that the current limitations may have converted the Internet in Iran from a household item perceived as a safe practice into a habit which requires risk-taking is alarming. To add to the extent of the challenge, the Iranian state media continually portrays the Internet as the cause of social and personal despair. Such circumstances do not constitute proper grounds for mass participation and involvement.

[240] *Arash Abadpour (2012) - "Booze, Drugs, and Blogs"*

The establishment of the national Internet may reduce this specific tension and yield a safer perception of this platform. Under the national Internet, accessing the web will in fact not constitute an illegal activity. This environment could provide more appropriate grounds for participation of the masses.

### Press the Button and Get Back to the Street

Involvement with the web, under the current conditions, is extremely time-consuming. Individuals have to wait for pages to load, for likes and comments to be posted, and for short videos to buffer. One may in fact estimate the amount of time wasted within the borders of Iran staring at a monitor and waiting for “Like” to transform into “Liked” through a lengthy and demanding process which may fail to succeed in the first few attempts. Given the argument that change happens in the physical world, and not on the shiny surface of monitors and smart phones, one should wonder how much more activity could have been possible if so much time had not been wasted on sending comments and liking posts.

The national Internet may in fact accelerate the process of participation in cyberspace. Individuals may in fact have the opportunity of becoming a user of the technology, as opposed to the spectators of gadgets and services. This trend may result in a more critical perspective on the role of the technology and how it can be more optimally used for social/political participation. In essence, individuals may have the time to attend a candle vigil, if the act of reading about the instances of violation of human rights would not require them to go through lengthy complicated steps of circumvention and trial and error.

### More People Talking about more Things

It could be argued that the hardship of using the web and the risks involved have resulted in what can be addressed as a bi-partitioning of the Persian language content on the web. On the one end, there is the community of activists who utilize cyberspace for their “causes”. The majority of the rest of the web, however, is utilizing it for one particular, yet common, application, i.e. easy pleasure. This includes Facebook pages with hundreds of thousands of likes and followers in which bits of nationalism, romance, lifestyle, “word of the wise”, and sexual fantasies are amalgamated into content which is posted, discussed, and shared widely. It is a matter of spending a few minutes before one would spot misogynistic, homophobic, chauvinistic, and even racist content circulating these spheres. One may argue that the Persian speaking cyberspace is being pushed into radicalism and extremism.

The Iranian national Internet may in fact reverse this process. By the fact that more people are going to be able to access the web free of the present hazards and worries can in fact result in conversations on issues of significance between members of the larger society. The average individual could in fact have the opportunity of listening to and having a voice in the discourse. The increase in the volume of interaction on the web could dissolve radicalism into practical ambition to change.

### Needle in the Hay

The national Internet needs to provide incentives for people to be willing to switch. These incentives could include higher connection speeds, more data allowances, and coverage of fast Internet in more geographical locations. Also, with the national Internet in place and operational, it would be harder for policy makers to make the case for keeping bandwidth low. As a result, the volume of traffic on the national Internet network will most likely be significantly higher than at the present time. The increase in the volume of activity on the web serves the activist community who will have better opportunities for escaping state monitors which will have their resources exhausted by the rest of the web.

One only needs to imagine the hike in the volume of data transfer when events of national significance occur. For example, in days prior to and after a soccer match between two well-known football teams, it is imaginable that the traffic on the web would virtually throttle the monitors. These days provide valuable opportunities for an activist who has, for example, a video that he or she wants to share. The upload stream of the video would be practically buried underneath the volume of conversation around the game. The activist could then succeed in uploading the video to several domestic video-sharing websites while everyone else is busy discussing the game. This imaginary strategy would reach its climax when the activist shares the link on a less busy day and could have access to a window of opportunity while the authorities are rooting out the video.

### Possibilities for "Accidental Exposure"

With more people on the line, the activist community has the possibility of utilizing flash mobs and other crowd-affecting tactics to communicate its message and share its content. In the post-national Internet era, one activist may choose to "accidentally" expose a video which discusses a case of human rights violation on a popular Facebook page, or whatever the "national Facebook" is going to be named. The vast audience of a Facebook page which contains fashion-related content may in fact one day wake up to a picture showing the harsh conditions of child factory workers in a province.

The national Internet can in fact provide for the Iranian activist community what the shopping mall has given their North American counterparts. There is no doubt that the state will set up the national Internet in order to advance its own narrative or at the least allow unthreatening content to circulate. The activist, however, will have the possibility of blending in with the crowd in order to walk into the mall and wait for the moment of opportunity, when he or she would step out, raise its voice, and then dive back into the crowd.

### Videos of Cats Flushing the Toilet, All Day Long...

The potential increase in bandwidth allows for the possibility of wasting it. In fact, activists generally do not need high bandwidth. Exceptions of course exist. For example, one activist may decide to share a video or an audio file. These types of content, however, can generally be transmitted through a few megabytes of data that can be trafficked through the web. Textual and pictorial content, on the other hand, require significantly less than that, with status messages occupying in hundreds of bytes. The fact of the matter is that the activist could utilize the high bandwidth communication lines in order to transmit her own messages without being noticed.

In one scenario, the activist would post a long video of a cat slowly flushing the toilet. The twenty-minute video, however, is essentially a cover, a waste of bits and bytes. The target, here an individual who has been given the heads-up, will be able to extract from the pile what he or she is looking for, i.e. the status message, the picture, the blog post, the video, or the audio file. The national Internet can in fact give birth to shadow networks which obfuscate communication. There will be people staring at irrelevant videos day long, whereas in fact the whole stream is ignored and the message is retrieved.

In the national Internet there could be innocent videos of cats and dogs playing around, or better, state figures giving speeches on the necessity of this and that, where the stream has in fact been contaminated with critical-to-state content. One person would be able to share the video of Mr. President giving a speech, knowing that the audience will in fact recognize that what they should be looking at is not Mr. President; it is what is being carried deeper in the stream. The activist community, in fact, may be capable of infecting the Iranian national Internet with critical content.

### How about Wikipedia?

The national Internet project may in fact elevate the sense of entitlement in the Iranian population. The possibility of accessing the web at higher speeds, comparable to what many in the rest of the world are capable of having access to, essentially could raise questions in the Iranian population on all the other things that they deserve and are deprived of. This process could be catalyzed through the establishment of the national Internet. This is a cost for the state apparatus. It is imaginable that when the national Internet is offered at a reasonable bandwidth, there will be follow-up questions on why a website such as Wikipedia is not accessible at similar speeds, for example. One would eventually ask the question, “isn’t accessing Wikipedia our right as well?”

### Let’s talk Business

Anecdotal evidence indicates that the frequent disruptions of connectivity in Iran and the slow bandwidth have had discouraging impacts on the relationship between Iranian businesses and the Internet. Entrepreneurs have the valid concern that if they create a business which heavily depends on the Internet, they would become dysfunctional when the Internet is slow and connection cannot be made. The national Internet project, however, can change this setting and may make the Internet more habitable for the businesses. Penetration of the Iranian cyberspace by prominent businesses could in turn act as a momentum against limitations and harsh treatments of the kind that the state has been practicing in the past two decades. With large entities conducting business online, there will be one additional factor for pressuring the Iranian government when policy-makers intend to impose limitations on connectivity. The state in fact would have more obligations to converse with these businesses, as it would not be able to label them as “counter-revolutionary” and “immoral agents” to distort the public opinion. Additionally, businesses could make the case that the restriction of online access can have a negative impact on their livelihood, which could be essential when taxation, unemployment, and other economic factors are discussed publically.

In effect, the national Internet project could add a heavyweight stake-holder to cyberspace. These entities, i.e. businesses, could in fact help social and political activists in securing the web for their narrative, although businesses in fact may not have any interest in being a helping hand.

### Innovating the Way Out

Any conversation about the Iranian cyberspace is inevitably limited by our understanding of the possibilities of this sphere in the current setting. In fact, future developments could reshape the Persian web into new concepts which are not imaginable at the present time. A faster, more accessible Internet can act as the test-bed for innovations that would allow the Iranian citizens to make use of this space in novel ways and in different forms.

What needs to be recognized is that the plea for change is an organic phenomenon, not an extrinsically imposed factor. Hence, it is imaginable that with the web becoming more accessible to the Iranian public, and with the groups and individuals with the capacity to innovate being present in this space, many opportunities would exist which are outside the realm of possibility and imagination at present.

« content

## Conclusions

The argument is that there are indications that this project could cause the establishment more harm than it may be evident upon initial glance.

This contribution discusses the possibility that the national Internet may in fact increase the volume of activity on the web. This phenomenon could then lead to an increase in the circulation of content produced by activists when a leak, either planned and intentional, or accidental and unintentional, occurs. The national Internet would eliminate the impression that activity on the web is an illegal act, something which this contribution argues increases lawlessness on the web and limits its use to fringe groups.

The current Internet status in Iran is wasteful. It is argued that active individuals spend time that they may utilize in other activities when they need to interact with the web. In essence, the cost of activity on the web in Iran at present time is unnecessarily elevated.

With more people becoming involved in more conversation, the national Internet may be less radicalized and activists may be able to carry out their activities and blend into the background more efficiently.

The state could have a more difficult time justifying its use of limiting factors when the population becomes accustomed to a faster web, and the business-friendly environment of the national Internet can encourage this sector to become a helping hand in fighting limitations on the Internet without the businesses having particular care for the cause of the activist community. Additionally, innovation would be more probable in the high speed national Internet. Some of these innovations may in fact be the last blow, not just on the national Internet, but the censorship apparatus of the regime as a whole.

The Iranian state has carried out its projects on the face of opposition from the Iranian activist community and external forces. The important point is to discover the possibilities in the post-national Internet era and to prepare for the capitalization of them. It is only through active exploitation of the national Internet that this project is going to fail.