# DIGITAL (IN)SECURITY IN IRAN


Volunteer Activists
PEACE | DEMOCRACY | HUMAN RIGHTS

# CONTENTS

# EXECUTIVE SUMMARY

Volunteer Activists
PEACE | DEMOCRACY | HUMAN RIGHTS

This report provides a deeper understanding of the difficult situation and constraints Iranian digital activists and civil society actors are faced with. It also presents the findings of a targeted and specially designed study for Iranian civil society organizations (CSOs) as well as social activists living and working in Iran. The findings of this project identify the training needs of CSOs and social activists in Iran, and the recommendations made are towards designing and compiling capacity building projects. The research for this study was done between November 2014 and February 2015 and is the first quantitative and qualitative research conducted in Iran after an eight-year period of confinement and suppression of local activists. It was carried out by Volunteer Activists, a non-profit organization that focuses on the promotion and expansion of democracy, the advancement of human rights and peace building in the Middle East with a particular focus on Iran.

## Digital Status Report

The Iranian government continues to block millions of websites that run counter to religious or political beliefs and in 2011 it became known that Iran had began building a National Information Network (NIN), or in other words an Iran-only internet, with it's own infrastructure that was completely isolated from the world wide web and would permit even tighter control over the flow of information. Approximately %50 of the world's top 500 visited websites are blocked in Iran, including Twitter, Facebook and Google Plus as well as other websites related to health, science, sports, news and even shopping. In fact, a study of 65 countries worldwide places Iran at the very last spot interms of internet freedom.

Iranian authorities pursue three main goals to prevent any form of cyber opposition.

1. The first goal is the development of NIN, which will make the state the sole "gatekeeper" of the internet.

2. The second goal is the continuing battle against "undesired" content and websites by filtering and blocking access to it - with an increased focus on mobile phone applications.

3. The third and final goal for the government is to better position itself to be able to legislate against and prosecute digital activists.

Despite these restrictions and the general environment of "insecurity", "the internet remains the only viable means for Iranian citizens and dissenters to obtain news and organize themselves. Traditional media outlets are tightly controlled by the authorities, and satellite broadcasting from outside Iran is subjected to heavy terrestrial jamming"1.

1 Freedom House (2014), Freedom on the Net 2014, www.freedomhouse.org. p2

# Digital Activism - A Needs Assesment

The civil activist space in Iran has become severely limited and dangerous since the disputed 2009 elections and the subsequent crack-down of the so called 'Green Movement'. As a result of the greater risks and more hostile environment, civic activism has gone 'underground' and now happens predominantly online - utilizing social media platforms, websites, email distribution lists, blogs, and conferencing software such as gotoMeeting or Skype.

One of the primary issues for digital activists is that digital technologies become part of their regular working practices (e.g. social media). However, the paradox is that as technologies become easier to use, they also become increasingly more difficult to control, thus reducing the number of endusers with the expertise to understand how they work, where information is stored, what data is collected, and who has access to it. This can be very dangerous and problematic as activists increasingly rely on mainstream tools because of their ease to use and broach reach. As such, the risks activists face is directly related to the choices they make as users which relies on the understanding and training they have to use such tools.

It is for this precise reason why first hand research was conducted to better understand the skills and capacities as well as needs of CSOs and digital activists.

## The key points this study found are:

- Iranian CSOs and activists view the internet as a crucial medium and as:
  - a source of up-to-date information, knowledge, research and know-how
  - a source for all types of resources (translated from English to Farsi)
  - a tool for independent inquiry
  - a tool to document and communicate real-time human rights violations as well as gain international support to curb injustices by the authorities
  - a major tool for resistance, activism and freedom of expression
- Primary concerns for Iranian digital activists are:
  - Severely reduced internet speeds
  - Filtered content (blocked websites and social media platforms)
  - Government surveillance and punishment (+ lack of digital security know-how)
  - Lack of access to ICT tools & equipment (expensive / sanctions)
  - Lack of ICT know-how (e.g. software and internet skills)
  - Specialised knowledge content (databases) is often only accessible in English or with credit card information (which Iranians don't have).

- The report also found that most people active in the digital space simply do not have an adequate knowledge about how to protect themselves when using online or voice communication.

- The survey revealed activists spend between 5-3 hours per day in social networks but at the same time, lack a basic understanding of how to act responsibly within social media networks. There is a great need for educating digital activists about social media, how to use it effectively, as well as how to use it responsibly.

- This study also revealed a paradoxical relationship between a majority of respondents being acutely aware of the threat environment in Iran but equally admitting that they are not taking proper measures to protect themselves. In many cases this is due to a rather large knowledge gap of basic ICT training amongst Iranian activist.

- Lastly, the survey revealed a great desire of Iranian digital activists to be engaged in more capacity building activities to strengthen their ICT skills.

RECOMMENDATIONS

The digital security discourse needs to move away from a techno-centric only conceptualization. Rather than focusing solely on software-based mitigations of digital security threats, which tend to age fast in a rapidly changing climate, activists need to be empowered to react quickly and flexibly. This implies a capacity building process, which would foster the development of critical thinking, agility and creative responses to digital security threats.

In this light, the report suggest a range of tools that are both technology-based as well as rely on capacity building approaches.

# INTRODUCTION

Volunteer Activists
PEACE | DEMOCRACY | HUMAN RIGHTS

## Purpose

The objective of this report is to provide a deeper understanding of the difficult situation and constraints Iranian digital activists and civil society actors are faced with. It also presents the findings of a targeted and specially designed study for Iranian civil society organizations (CSOs) as well as social activists living and working in Iran.

The present research has been conducted as part of the organizational mission of the Volunteer Activists (VA) Institute. The findings of this project identify the training needs of CSOs and social activists in Iran, and the recommendations made are towards designing and compiling capacity building projects. The Volunteer Activists Institute aspires to assist activists and CSOs in Iran during this transition period, by implementing plans for efficient capacity building, so that they can respond to the needs of their stakeholders, and contribute to the development and democratization of Iranian society and the Middle East region.

# DIGITAL (IN)SECURITY IN IRAN

Volunteer Activists
PEACE | DEMOCRACY | HUMAN RIGHTS

# INTERNET FREEDOM - A BRIEF GLOBAL BACKGROUND

In 2011, the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank William La Rue, submitted a report to the UN Human Rights Council, which "explores key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet"2. The report assessed the current situation of global internet freedom, highlighting concerns and restrictions, and made concrete recommendations how to further strengthen the principles of internet freedom as an effective tool for the human right to freedom of opinion and expression. Some observers have suggested that La Rue goes as far as declaring internet access as a fundamental human right3, and denial of access to it, a human rights violation4.

La Rue states that
"by vastly expanding the capacity of individuals to enjoy their right to freedom of opinion and expression, which is an "enabler" of other human rights, the Internet boosts economic, social and political development, and contributes to the progress of humankind as a whole."5

He further emphasizes that
"there should be as little restriction as possible to the flow of information via the Internet, except in few, exceptional, and limited circumstances prescribed by international human rights law."6

Moreover,
"the full guarantee of the right to freedom of expression must be the norm, and any limitation considered as an exception, and that this principle should never be reversed."7

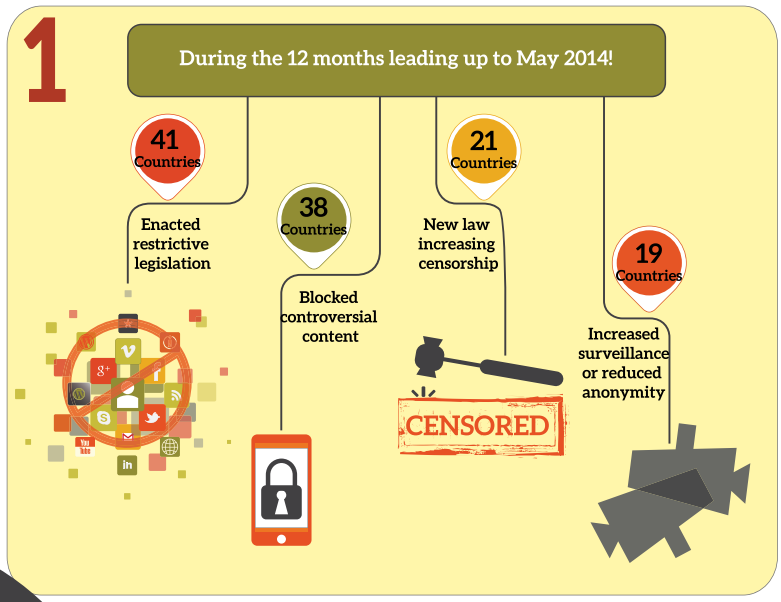
It is against this background that this report attempts to highlight some of the trends and concerns of internet freedom today before focusing exclusively on the situation in Iran.

---

2 Frank William La Rue (May 2011), United Nations, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, p.1, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
3 Jenny Wilson (7 June 2011), TIME, http://techland.time.com/07/06/2011/united-nations-report-declares-internet-access-a-human-right/
4 David Kravets (3 Jun 2011), Wired, http://www.wired.com/06/2011/internet-a-human-right/
5 Frank William La Rue (May 2011), Ibid, p.19
6 Frank William La Rue (May 2011), Ibid, p.19
7 Frank William La Rue (May 2011), Ibid, p.19

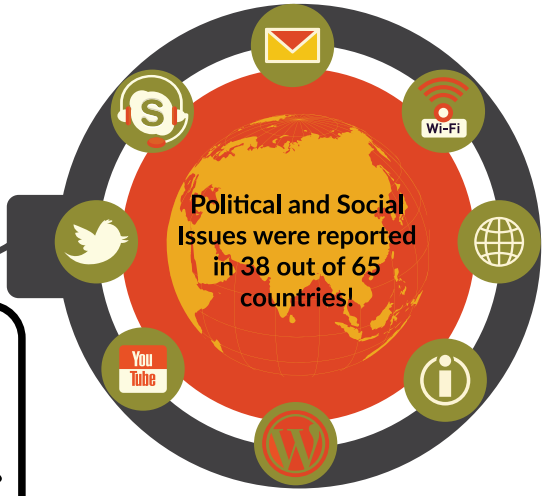
Freedom House in its study “Freedom on the Net 2014”, which analyses 65 countries, reports that internet freedom is declining for its 4th consecutive year. The report attributes this decline predominantly to three key developments8:

During the 12 months leading up to May 2014, 41 countries passed or proposed legislation to limit or punish forms of speech online, increase government surveillance mandates or increase their powers to control online content.




2

Since May 2013, arrests for online communications regarding politics and social issues were reported in 38 out of 65 countries. This number is especially high for the Middle East and North Africa region where arrests were documented in 10 out of the 11 countries that were searched.




3


Independent news/media websites were harassed considerably more and many citizen journalists were attacked while reporting on the conflict in Syria and anti-government protests in Egypt, Turkey and Ukraine. Governments also increased their licensing and regulation for web platforms to make it more difficult.

8 Freedom House (2014), Freedom on the Net 2014, https://freedomhouse.org/report/freedom-net/freedom-net2014-

In addition, the report9 also identified three emerging threats which increasingly threaten the rights of internet users globally. They are:


Requirements for data localizations for private companies to maintain data storages within countries are increasing. This is largely due to the fact that governments wish to bring international web companies under domestic jurisdiction following the NSA revelations around Edward Snowden. These developments could expose user data to local law enforcement.


Rights of lesbian, gay bisexual or transgender men and women are more and more threatened by digital harassment and bullying. This has led to a form of are undermined self-censorship that prevents their authentic participation in online culture.

3

Cybersecurity is decreasing as government opponents and human rights defenders are increasingly attacked by sophisticated and targeted cyber attacks as reported in 32 of the 65 countries examined.


Also a report by Hankey and Ó Clunaigh confirms that attacks on human rights defenders "have escalated over the past two years, with a significant increase in the number of entrapments and networks being compromised through the use of computers, cameras, mobile phones and the internet"10. Their report also states that there is a growing concern about these new threats for activists as well thinking about how best to enable digital human rights defenders to assess and mitigate the related risks.

Nevertheless, spurred by the NSA revelations of Edward Snowden, internet security and the right to online privacy has received a tremendous awareness boost and been subject to public debates on or offline. Threats previously only considered by a minority (tech industry professionals) have now been pushed into the limelight and governments are increasingly subject to pressure by civil society actors and ordinary users to better and - more importantly - transparently legislate internet freedom, digital security and online privacy.

---

9 Freedom House (2014), Ibid.
10 S. Hankley & D. Ó Clunaigh (2013), Rethinking Risk and Security of Human Rights Defenders in the Digital Age, Journal of Human Rights Practice Vol. 5 | Number 3 | November 2013 | p. 536

# INTERNET FREEDOM IN IRAN

Digital Status Report

It is well-known that freedom in Iran - when defined in democratic terms - is an aspiration that still requires much work. Ever since the so-called Islamic revolution in 1979, during which the Islamic Republic of Iran was declared (following a referendum in which apparently %98 of people voted for this system), political power was concentrated in the Islamic Revolutionary Council which was dominated by hard-line religious fundamentalists. Since then, the Iranian regime has had a long history of violently cracking down any form of regime opposition or any other 'non-conformant' opinion and action - whether religious, social or political. This is true for the offline as well as the online world.

The digital revolution in Iran began in the 1990s to reinvigorate technological and scientific progress in an economy that had been severely stunted following eight years of war with Iraq. As such, the private sector was the main driver of internet development until the year 2011. Under reformist president Mohammad Khatami (-1997 2005) this changed when the government began to heavily invest in Information & Communication Technology (ICT) infrastructure but also started restricting the new communication channels by keeping a lid on the newfound freedom of online expression12. At the same time, Supreme Leader Ali Hosseini Khamenei, who arguably holds more power and influence than the president, first took "control" of internet freedom in Iran in 2001, when he - by decree - ordered that all Internet Service Provider (ISP) connections to the international internet must become centralized13.

Thereafter in 2005, internet filtering became a common practice and intensified severely since the disputed presidential elections in 2009. The government has and continues to block millions of websites that run counter to religious or political beliefs and in 2011 it became known that Iran had began building a National Information Network (NIN), or in other words an Iran-only internet, with it's own infrastructure that was completely isolated from the world wide web and would permit even tighter control over the flow of information14. NIN would allow the government to be the sole "gatekeeper" of the internet and also make the government the provider of SSL security certificates - practically giving government authorities the ability of undetectable access into anyone's accounts15. The development of NIN also entails developing a national internet browser as well as a national operating system. This makes it very clear that the Iranian government is building a wall around

11 Freedom House (2014), Freedom on the Net 2014, www.freedomhouse.org, p.2

12 Freedom House (2014), Ibid., p.2

13 Freedom House (2014), Ibid., p.2

14 Washington Post (2012), Iran preparing internal version of internet, http://www.washingtonpost.com/world/national-security/iran-preparing-internal-version-of-internet/-79458194/19/09/2012 01c11-3e-2b32-260f4a8db9b7e_story_1.html

15 International Campaign for Human Rights in Iran (2014), Internet in Chains, p. 9

the international internet whilst positioning itself to manage the only access points to it or whilst providing government-developed alternatives altogether.

%50 of the world's top 500 visited websites are blocked in Iran.

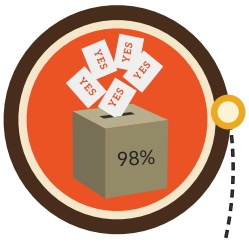
The prospect of state-authored SSL security certificates is especially worrying. When provided by a neutral or legitimate source, SSL certificates provide a decent level of security, but when provided by state organizations, it not only gives the government potential access to all online activity and full access to visited or created content, but it also provides the illusion of online security. This becomes especially true when a large number of users start using the state's SSL certificates as this will turn the default browser warning of an "untrusted" SSL certificate source to a "trusted" one. When this happens SSL certificates receive "root" certification and are considered safe giving many users the illusion of online security16. This process will be achieved by promoting Iranian SSL certificates via the national Iranian browser Zaina and via the national Iranian operating system Zamin until usage has resulted in the desired root certification declaring Iranian SSL certificates as "trusted". To ensure the usage of Zaina and Zamin the government decreed in 2013 that all Window's based systems need to move to Linux which would host the new system17. Again, it is unknown to what extent progress has been made but it is known that progress is behind schedule. Officials excused the accelerated development and significant investments into infrastructure and security for NIN by declaring that cyber attacks aimed at Iran's nuclear program, such as Stuxnet, were increasing. However, there are reported (albeit not confirmed) plans to go even further that would see engineers develop and build a system that would identify any individual in Iran who goes online18. If such plans were realised it would mark the end for web anonymity altogether and be an even more severe threat to internet freedom than the already existing government surveillance or filtering measures. The presumed two-fold tactic of the Iranian government is simple yet effective. The removal of web anonymity scares and thus prevents users to access "questionable" online materials. Those that still do will be identified and punished which in turn scares other users to access such materials in the first place. However, it is not clear when NIN will be fully operational. In it's -5year development plan (2015 -2011), NIN is expected to be developed and ready for widespread deployment by the beginning of 2016 but several delays have

16 Int. Campaign for Human Rights in Iran (2014), Ibid., p. 10

17 Int. Campaign for Human Rights in Iran (2014), Ibid., p. 10

18 I. Lunden (2014), Report: Iran Developing System To ID Any Internet User, TechCrunch

# 1979
## Islamic Revolution!





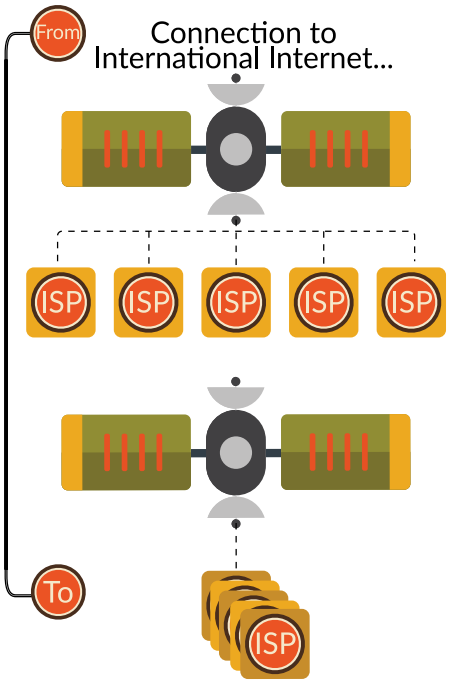

violently cracking down any form of regime opposition!


# 1990s
## Digital Revolution!

1997-2005


Restricted Communication by Controling Freedom House!

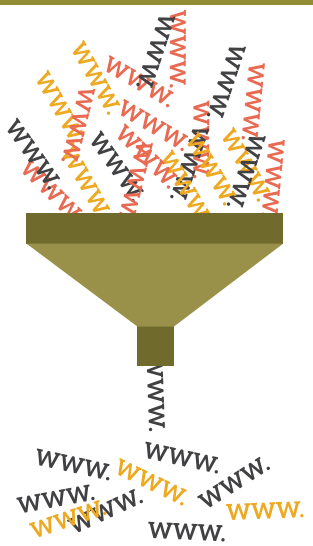
# 2001
## Supreme Ledaer took "control" of internet freedom in Iran!



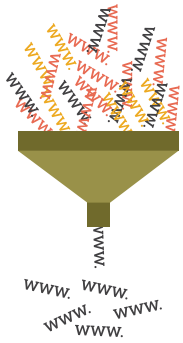

...MUST BE CENTRLIZED!

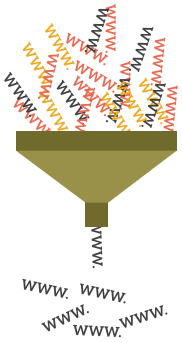
# In 2005

Internet Filtering became a common practice!



## 2009
**Presidential Election!**



**Internet Filtering became severe!**

**Government continues to block millions of websites!**

## 2011
**Building a National Information Network (NIN)!**




**50 % of the world's top 500 visited websites are blocked in Iran!**

been reported in recent years. Nevertheless, it is clear that NIN has remained a government priority and that work on it's implementation has steadily continued.

What is also clear, is best summarized the International Campaign for Human Rights in Iran:

once it (NIN) is fully implemented, all Internet access in Iran will take place through channels accessible to the state, state agencies will have access to all communications inside Iran on the National Internet, the authorities will be able to cut off access to the global Internet at will, and they will also be able to deny or limit access by Internet users abroad to content in Iran's domestic Network.[19]

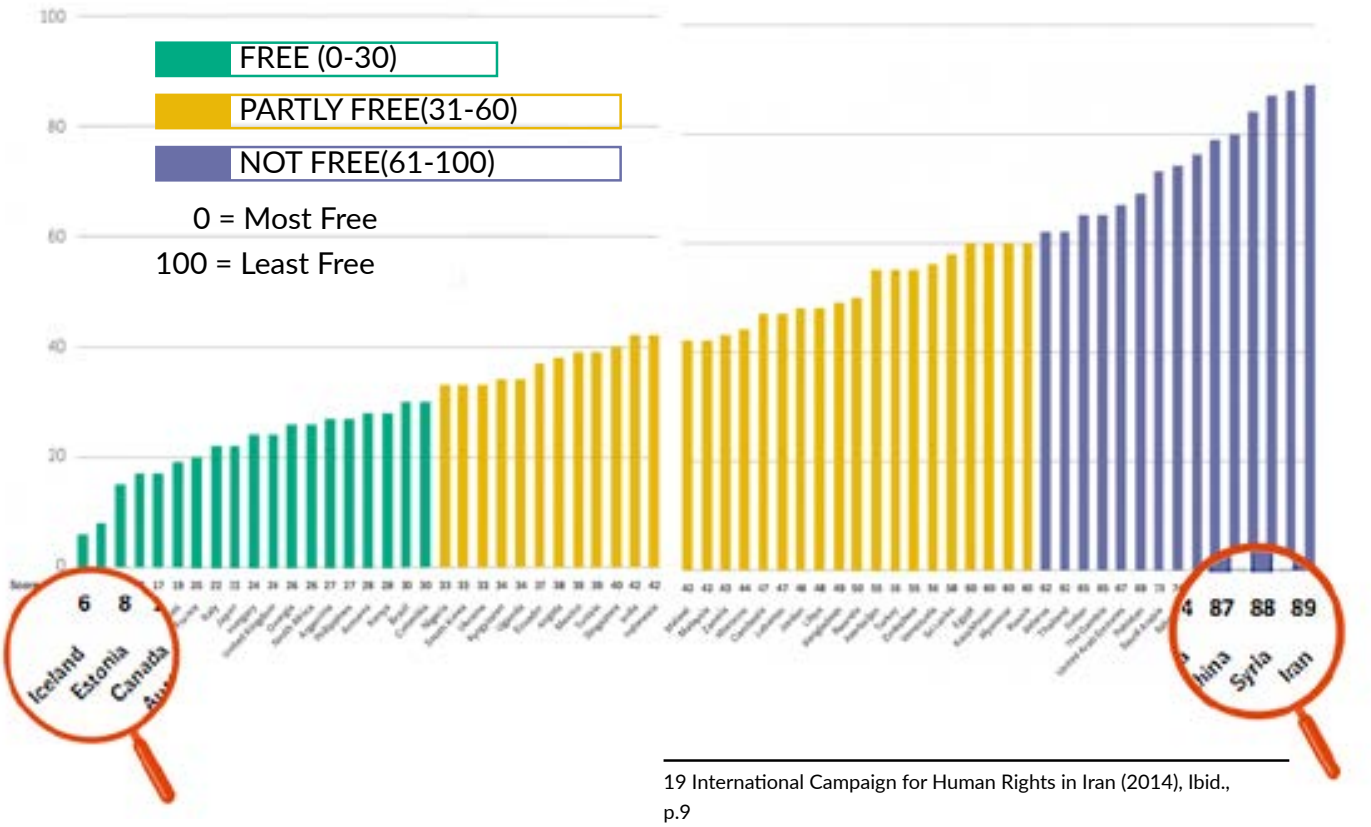
Despite these truly frightening prospects, one cannot be complacent about the already existing crackdown of internet freedom in Iran. Ahmed Shaheed, UN Special Rapporteur on the human rights situation in Iran, cites a study which found

Freedom on the Net measures the level of internet and digital media freedom is 65 countries. Each country recieves a numerical score from 0(the most free) to 100(the least free), which serves as the basis for an internet freedom status designation of FREE(0-30 points), PARTLY FREE(31-60 points), or NOT FREE(61-100 points), Ratings are determined through an examination of three broad categories:

**A. Obstacles to Access:**
Assesses infrastructural and economical barriers to access; governmental effects to block specific applications or technologies; and legal regulatory, and ownership control over internet and mobile phone access providers.

**B. Limits on Content:**
Examines filtering and blocking of websites; other forms of censorship and self-censorship; mainipulitaion of content; the diversity of online news media; and usage of digital media for social and political activism.

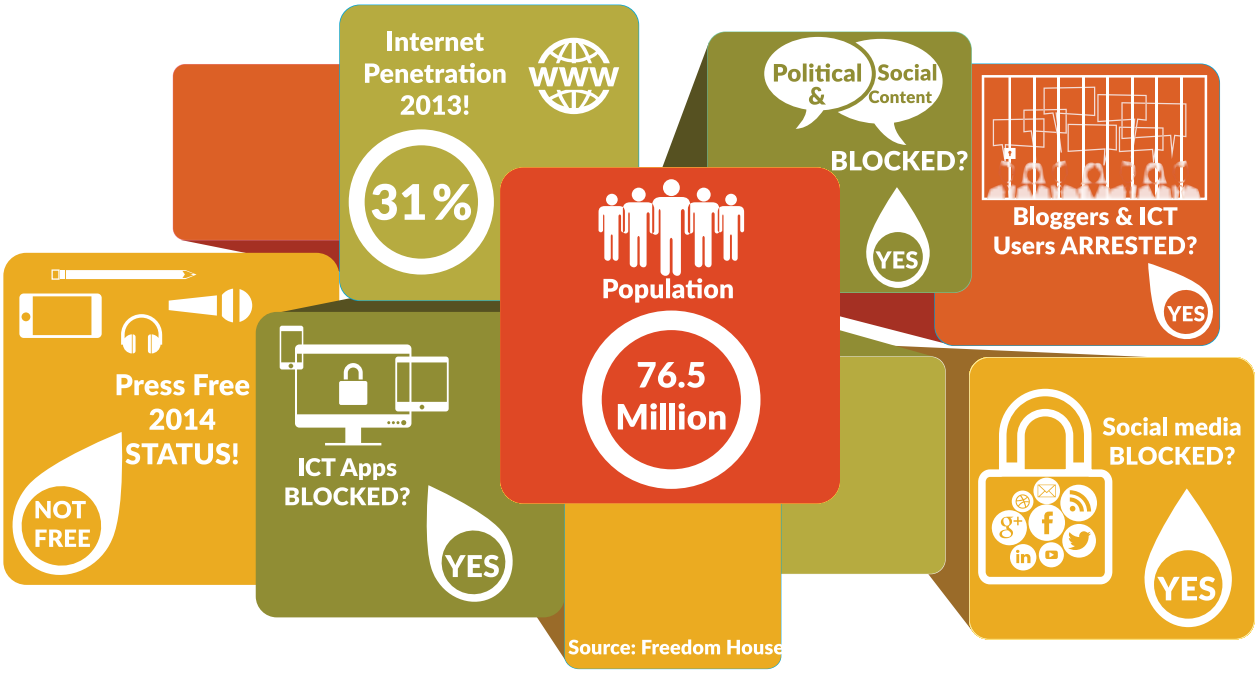
**C. Violations of User Rights:**
Messures legal protections and restictions on online activity;Surveillance, privacy, and reprecussions for online activity, such as legal procecution, imprisonment physical attacks, or other forms of harrassment.

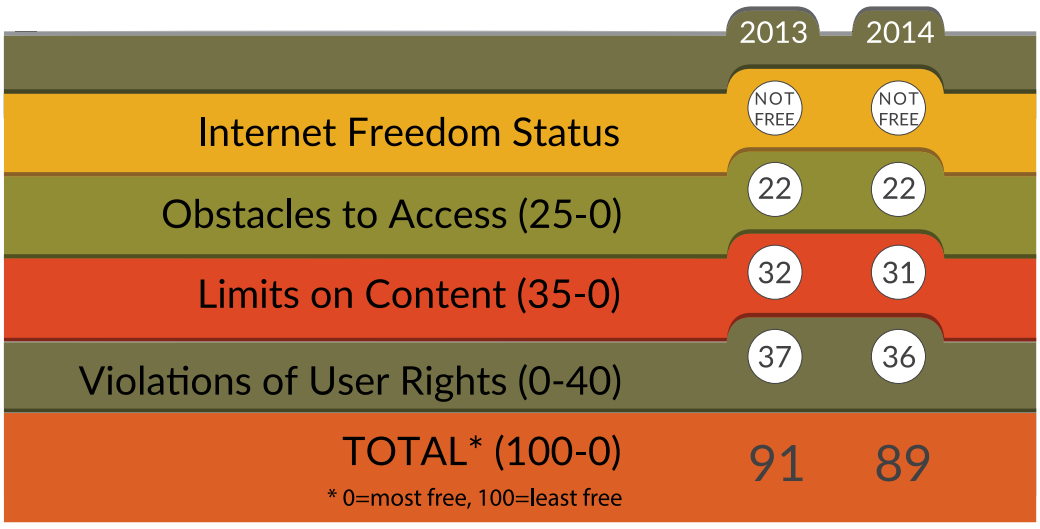



19 International Campaign for Human Rights in Iran (2014), Ibid., p.9

that approximately50% of the world's top 500 visited websites are blocked in Iran, including Twitter, Facebook and Google Plus as well as other websites related to health, science, sports, news and even shopping[20]. In fact, the study of 65 countries worldwide places Iran at the very last spot in terms of internet freedom. The rank given to each country is determined by a score that measures a) obstacles to access, b) limits on content and c) violations of user rights. Out of a score between 0) 100-0 being most free and 100 being least free), Iran received a score of 89 for 2014.

Iran also ranks quite low for general internet speed, placing at rank 156 out of 192 countries. Moreover, it has the lowest average peak connection speed in the world. Shaheed concludes that "Internet speed is intentionally reduced to frustrate users and limit communication"[21].




20 Ahmed Shaheed (2014), Layers of Internet Censorship in Iran, http://shaheedoniran.org/english/blog/layers-of-internet-censorship-iniran/
21 Ahmed Shaheed (2014), Ibid.

He also states that:

> Internet traffic and speeds dropped significantly in the days following the 2009 Iranian presidential election and in the weeks leading up to the 2013 election. Throttling has also been noticeable during times of international political upheaval, including during the Arab Spring.[22]

Nevertheless, some observers have raised their hopes following the 2013 election of President Hassan Rouhani as he and his government are widely viewed as being on the more moderate/liberal side - especially when compared to his predecessor Mahmud Ahmadinejad. Mr Rouhani, for example, Ahmed Shaheed (2014), Ibid. hinted at several occasions that he intends to lift some of the internet restrictions that criminalize many of the estimated 30 million Iranians who go online.[23] "Mr Rohani's culture minister, Ali Jannati, has gone further, likening the current restrictions to the ban on fax machines, video recorders and video tapes that followed the Islamic revolution of 1979, an action he described in March as—in hindsight—"ridiculous"[24]. Further, a majority of Mr Rouhani's cabinet ministers have opened up social media accounts despite the fact that Twitter and Facebook remained blocked.[25]

However, the fact that after 1.5 years in office, Mr. Rouhani and his government have not managed to bring about any major changes to the internet situation in Iran, speaks to the complex political system of interwoven institutions in the country. One could also make the case that in light of the arguably more powerful, and by default more hardline religious institutions, such as the Guardian Council, the Supreme Leader and especially the Revolutionary Guard, the Presidency and government's powers appear quite limited and continue to be opposed by the more traditional and hardline oriented religious institutions. For example, on 1st October 2014, Entekhab - a news website close to president Rouhani - was blocked without any explanation[26]. Six days later on 7th October MP Ali Motahari announced that the blocking of the Entekhab was illegal as it was based on a "personal decision" rather than subject to due legal process. To further demonstrate President Rouhani's and his government's lack of political capital - despite good intentions - it should be noted that under his rule, widespread filtering and the blocking of social media tools and mobile apps remain in place, the implementation of NIN has been considered a priority by the government and its development has been sped up, and lastly a significant number of Iranian bloggers, techies and digital activists have been arrested for online activities and received heavy prison sentences[27].

22 Ahmed Shaheed (2014), Ibid.
23 The Economist (2014), Iran's internet politics - everyone's doing it, 19 Jul 2014 http://www.economist.com/news/middle-east-andafrica/-21607894liberals-and-conservatives-argue-over-restrictionsinternet-everyones-doing
24 The Economist (2014), Ibid.
25 Freedom House (2014), Ibid., p.2
26 Small Media (2014 /10), Iranian Infrastructure and Policy Report, p.8 http://smallmedia.org.uk/sites/default/files/u8/IIIP_Oct14.pdf
27 Freedom House (2014), Ibid., p.2

Moreover, on 9th November 2014, ICT Minister Mahmood Vaezi said that the current Internet speed restrictions for domestic users will remain in place until NIN is launched.[28]

In summary, it can be argued that Iranian authorities pursue three main goals[29] to prevent any form of cyber opposition. The first goal is the development of NIN, which will make the state the sole "gatekeeper" of the internet. The second goal is the continuing battle against "undesired" content and websites by filtering and blocking access to it - with an increased focus on mobile phone applications. The third and final goal for the government is to better position itself to be able to legislate against and prosecute digital activists. In essence it is exactly as described by Hankley & Ó Clunaigh (2013), namely that information flows have always been—and probably always will be—a key target for those interested in undermining the work of digital activists.[30] Iran is a textbook case example for this. Despite these restrictions and the general environment of "insecurity", "the internet remains the only viable means for Iranian citizens and dissenters to obtain news and organize themselves. Traditional media outlets are tightly controlled by the authorities, and satellite broadcasting from outside Iran is subjected to heavy terrestrial jamming"[31]. However, as long as authorities view the internet as a security threat and continue to favor a militarized approach of regulating access to it, Iranian civil society has little chance to gain any type of internet freedom whatsoever.

28 Small Media (2014 /11), Iranian Infrastructure and Policy Report, p.8 http://smallmedia.org.uk/sites/default/files/u8/IIIP_Nov0_14.pdf

29 International Campaign for Human Rights in Iran (2014), Ibid., p.9

30 S. Hankley & D. Ó Clunaigh (2013), Ibid, p. 537

31 Freedom House (2014), Ibid., p.2

**1** Five youths and one director were arrested for a homemade video showing Iranian men and woman dancing together in a violation of conservative customs. The video was set to the lyrics of the Pharrell Williams song "Happy" which has been reproduced around the world. They received suspended sentences of 91 lashes and six months in prison, with the exception of Reyhaneh Taravati, who received a suspended twelve-month prison sentence in addition to the suspended lashes, provided they do not engage in any "wrongdoings" during the next three years.[32] The group was also forced to repent on state television.

**2** On December 2013 ,3, officials from the Revolutionary Guards arrested 16 digital activists in the southern province of Kerman, including eight staff members from the gadget review site Narenji.ir or its sister sites: Aliasghar Honarmand (Narenji's founder), Abbas Vahedi, Hossein Nozari, Reza Nozari, Amir Sadeghpour, Mehdi Faryabi, Ehsan Paknejad, and Malieh Nakhei. Referencing their apparent links to the BBC and BBC Persian, they were accused of being in contact with "enemy media" and "running a number of projects and plans for anti-revolutionary Iranians based abroad" according to a local justice department official. At least one individual had participated in or led BBC-funded journalism workshops, which officials linked to British intelligence. Five individuals were kept in solitary confinement for four months and subject to daily interrogations. In June 2014, the revolutionary court in Kerman sentenced 11 individuals for "designing sites… for media hostile to the regime": Honarmand to 11 years' imprisonment, Vahedi (2.5), Hossein Nozari (7), Paknejad (5), and seven others to 1.5 years plus 3 years' probation.[33]

**3** A Tehran revolutionary court passed long jail terms on seven Majzooban Nor contributors on 13 July on charges of anti-government propaganda, insulting the Supreme Leader and endangering national security. Hamidreza Moradi was sentenced to ten years in prison, Reza Entesari was sentenced to eight and a half years, and Mostafa Daneshjo, Farshid Yadollahi, Amir Islami, Omid Behrouziand

32 International Campaign for Human Rights in Iran (2014), Happy Video Youths Receive Suspended Flogging and Prison Sentences, http://www.iranhumanrights.org/09/2014/happy-sentenced/

Afshin Karampour were each sentenced to seven and a half years. The court also banned all of them from practicing any kind of political or journalistic activity during the first five years after their release. The defendants, who had been held in Tehran's Evin prison since September 2011, and their lawyers refused to attend the trial on the grounds that it was unfair.[34]

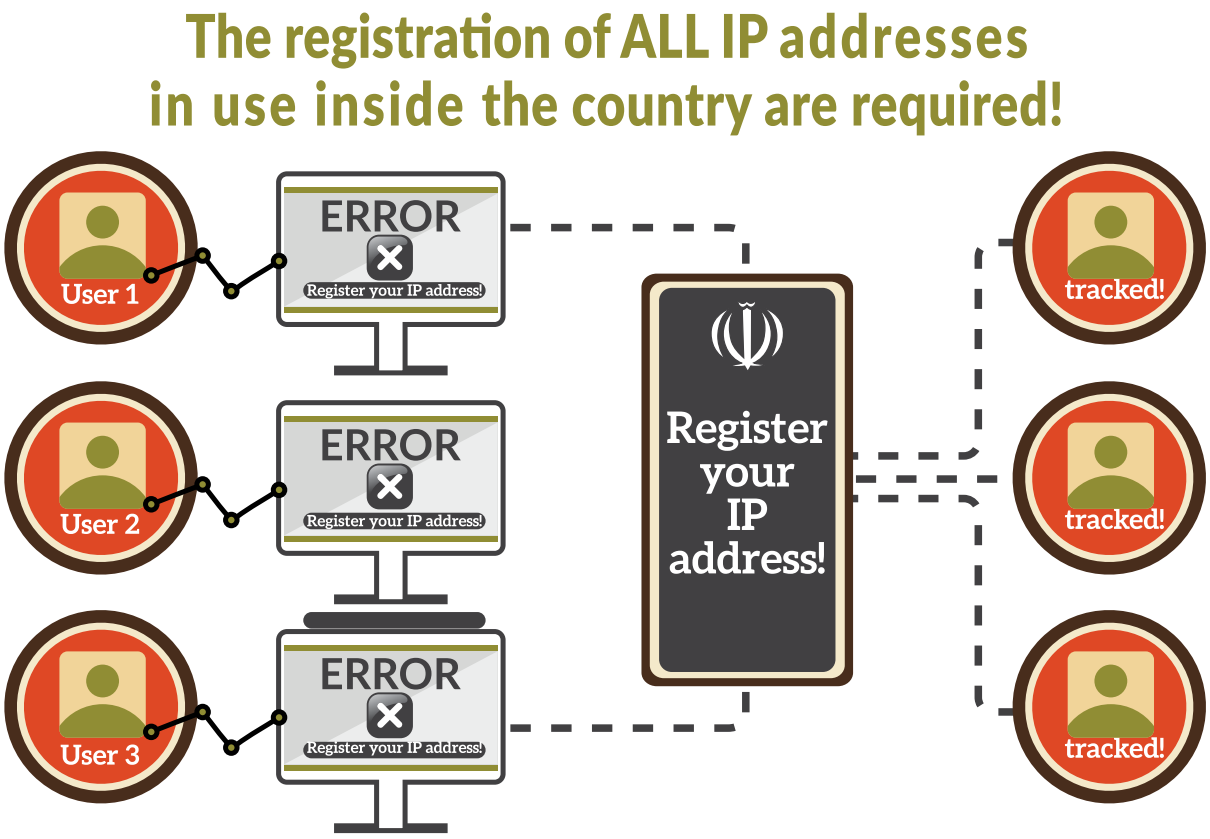
**4** Reporters Without Borders also reported that Revolutionary Guards arrested five young netizens– Roya Irani, Amir Golestani, Fariborz Kardar, Massoud Ghasemkhani and Seid Massoud Seiad Talebi – in early September. Charged by the Tehran prosecutor's office with "meeting to conspire against national security," they are still being held in Section 2A of Tehran's Evin prison and, according to the information obtained by RWB, are being subjected to a great of pressure to make confessions that can be used against them in a trial.[35]

**5** In a separate development from May 2014, eight individuals found guilty of blasphemy, spreading anti-regime propaganda, or insulting Supreme Leader Khamenei on Facebook and were sentenced between 7 and 20 years of jail time. Among those sentenced to 20 years was Roya Saberinejad Nobakht, a -47year-old woman and British national.[36]

33 Freedom House (2014), Ibid., p.11
34 Reporters Without Borders (2013), Rouhani's first 100 days see no progress on freedom of information, http://en.rsf.org/iran-rouhani-sfirst--100days-see-no2013,45474-11-19-.html
35 Reporters Without Borders (2013), Press Freedom Violations Recounted in Real-Time (Jan-Dec 2013), http://en.rsf.org/iran-pressfreedom-violations-recounted2013,43862-12-20-.html
36 Freedom House (2014), Ibid., p.11

## A Vague Legal Framework

Iranian authorities restrict access to online content which is considered anti-islamic or anti-regime while basing their actions on a legal framework which is not clearly defined and open to much interpretation by religious and judicial professionals. Whereas the Iranian constitution allows limited freedom of opinion and expression, the many irregularly enforced and vaguely worded laws restrict even those limited constitutional rights. The 2000 Press Law, for instance, prohibits the publication of thoughts, ideas or opinions that are misaligned with Islamic principles or are harmful to public rights.37 The 2009 Computer Crime Law, which makes service providers, such as web or blog hosting platforms legally responsible for any content posted on their sites38 and requires all Iranian Internet Service Providers to record all the data exchanged by their users for a period of six months, also forbids the publishing of materials deemed to damage "public morality and chastity" or to be a "dissemination of lies"39. Punishments for breaking these vaguely worded legislations range from small fines and prison sentences to draconian fines, long prison sentences and even the death penalty. This gives authorities a wide spectrum of legal interpretation as well as much flexibility when it comes to sentencing.




Further, the Iranian Communications Regulatory Authority issued Bill 106 in March 2012 which requires the registration of all IP addresses in use inside the country.40 Not

37 Freedom House (2014), Ibid., p.11
38 Article 2013) 19), Computer Crime in Iran: Online Repression in Practice 2013, p.13 http://www.article19.org/data/files/medialibrary/37385/Computer-Crimes-in-Iran-.pdf
39 Iranian Human Rights Documentation Center, Islamic Republic of Iran: Computer Crimes Law, http://www.iranhrdc.org/english/human-rights-documents/ngo-reports/article-19/1000000084-islamic-republic-of-iran-computer-crimes-law.html

40 Freedom House (2014), Ibid., p.13
41 Radio Free Europe Radio Liberty (2012), Iran Announces New Restrictions For Internet Cafes, http://www.rferl.org/content/iran_announces_new_internet_restrictions/24442396.html

only is this a fundamental objective for the NIN rollout but it will also allow authorities to identify and track digital users quicker and more effectively. Moreover, since March 2012, cybercafes, which are a very large internet access point for Iranians, are required to obtain their user's names, father's name, national ID number and telephone number before allowing them to use one of their computers. In addition, cybercafe owners are also required to install closedcircuit surveillance cameras and retain the video footage as well as user browsing history for six months.41 Similar requirements are present for mobile telecommunications as well. Identification is required of anyone purchasings mobile phone subscriptions or pre-paid SIM cards allowing the authorities to identify the sender and receiver of any message sent (voice call or SMS).

Moreover, in an effort to show that content filtering is based on a legal framework, institutions to oversee internet filtering, such as the Committee in Charge of Determining Unauthorized Websites, have been been created.

However, Freedom House notes that:

> owners of websites registered with the Ministry of Culture have complained that they received no explanation when their websites were filtered. The authorities claim there is a procedure for disputing filtering decisions. However, the process is highly inefficient, and even conservative bloggers have failed to have their web pages unblocked by lodging complaints. Moreover, the dispute process requires the website owner to disclose his or her personal information and accept responsibility for any misconduct in the future, a commitment that few are willing to make given the risk of severe punishment.[42]

Iran's Supreme Leader Khamenei also issued a decree in March 2012 to establish the Supreme Council on Cyberspace (SCC) - a centralized institution for policy making and regulation of Iran's virtual space43. This decree effectively removed the authority over this space from the executive, legislative and judiciary branches of government and brought it under direct control of the Supreme Leader himself. Not only is this move politically motivated but also economically. By controlling the virtual space, the Supreme Leaders wields a lot of economic power. For instance, on 1st December 2014, "Deputy ICT Minister Aliasghar Amidian said 18 companies applied for Internet Protocol Television (IPTV) licenses. He announced that the ICT Minister was unable to grant them licenses because the Supreme Council of Cyberspace (SCC) had not provided the required permission".[44]

42 Freedom House (2014), Ibid., p.8
43 Freedom House (2014), Ibid., p.5
44 Small Media (2014 /12), Iranian Infrastructure and Policy Report, p.7 http://smallmedia.org.uk/sites/default/files/u8/IIIP_Dec2014.pdf

## International Sanctions and its Effects for Digital Activists!


International sanctions constitute another considerable obstacle - not just for digital activists but also for the whole of Iran's ecosystem. For instance, sanctions prevent Iranians from making use of common international payment systems such as Visa or Mastercard. This makes transferring money to and from Iran expensive and risky, as Iranians must use middle men (brokers) rather than banks. Also transferring money into Iran is risky and in some cases impossible due to international sanctions. This makes finding foreign investors nearly impossible because foreigners fear the added risks. Small Media reports that, anonymous Iran-based entrepreneurs have stated that securing foreign investment carries a number of personal security risks.[45] For instance, if Iranians accept money from foreign investors, they put themselves at risk as the authorities can easily accuse any Iranian accepting money from foreign sources as working for the "enemy". As such, they would risk heavy jail sentences due to charges of espionage and "accepting money from Iran's enemies".

45 Small Media (2014 /11), Ibid., p.4

Nonetheless, international sanctions also affect digital activists more directly. One of the bigger concerns is that Iranian activists often have to use outdated software because their Iranian IPs are blocked by many western companies e.g Java or Adobe. This results in Iranians not being able to benefit from security patches or updates and leaves their software and computers highly vulnerable to attacks from in or outside the country. Oracle is another major example of this. As one of the largest software retailers (after Microsoft), Oracle software is much used in businesses and organisations (project management


software, database managements systems or CRMs). When Oracle decided to block Iranian IPs in 2013 in compliance with U.S. law (following stricter sanctions), Iranian users were unable to update their software packages any longer (by conventional methods). This left many Iranian servers and systems exposed and vulnerable to zero-day and breaking exploits.[46]

But also access to knowledge generating sites such as the popular e-learning site Coursera is blocked under U.S. sanctions law.[47] Whereas this may not have any direct security impact, it does prevent Iranians from educating themselves.

46 Johna Casaretto (2013), SiliconAngel, Oracle blocks Iran Trafic, http://siliconangle.com/blog/27/03/2013/oracle-blocks-iran-traffic/

## Technologies & Strategies for Censorship and Surveillance

Irregardless of international legal restrictions prohibiting the sale of surveillance equipment and technology to Iran, there have been reports of Chinese and some Western companies providing the required technology for the Iranian authorities to monitor their citizen's digital presence.
In fact, it is claimed by some that the surveillance technology industry is the new arms trade48 - if it is lucrative and in demand then ways around sanctions will be found.
Reports by Reuters and the Wall Street Journal name Huawei Technologies and ZTE Corporation as key providers of surveillance technology to Iran - a report which both companies deny.[49]
The Reuters report states:

> Documents seen by Reuters show that a partner of China's Huawei Technologies Co Ltd offered to sell a Huawei-developed "Lawful Interception Solution" to MobinNet, Iran's first nationwide wireless broadband provider, just as MobinNet was preparing to launch in 2010. The system's capabilities included "supporting the special requirements from security agencies to monitor in real time the communication traffic between subscribers," [50]

Additionally, an uncovered Huawei power presentation details how it's technology would give Iranian authorities the ability for deep packet inspection (DPI), real time monitoring of communication traffic, the ability to block websites, track users and reconstruct email messages as a means of monitoring Iranian citizens.[51] Reuters also reported in March 2012, that China's ZTE Corporation had sold Iran's largest telecom firm a DPI-based surveillance system that was capable of monitoring landline, mobile and internet communications.[52]
Surveillance is not really secret in Iran. In fact, authorities have been quite transparent about their surveillance capabilities - most likely as a deterrent tactic. For example, it was officially confirmed that the content of SMS is subject to filtering when in June 2013 the director of the SCC stated that it will draft a new bylaw - together with the Ministry of Culture and Islamic Guidance - for monitoring the content of mass and promotional text messages.[53] In addition, the Communications Regulatory Authority (CRA) has provided regulations that all commercial SMS senders must submit the content of each SMS or service to the CRA for review prior to sending.[54] Moreover, ICT Minister Mahmood Vaezi officially stated on 18 November 2014 that Iran's government monitors all Iranian and non-Iranian mobile communication apps.[55]

47 Coursera (2015), https://learner.coursera.help/hc/en-us/articles/-201223869Age-Country-Restrictions
48 S. Hankley & D. Ó Clunaigh (2013), Ibid, p. 538
49 Freedom House (2014), Ibid., p.13
50 Steve Stecklow (2012), Reuters, Special Report: How foreign firms tried to sell spy gear to Iran, http://www.reuters.com/article/05/12/2012/us-huawei-iran-idUSBRE8B409820121205
51 Steve Stecklow (2012), Ibid.
52 Steve Stecklow (2012), Ibid.
53 Freedom House (2014), Ibid., p.9
54 Freedom House (2014), Ibid., p.9
55 Small Media (2014 /11), Ibid., p.8

On 6th December 2014, Vaezi held a press conference, stating that the government is ensuring that there will not be any kind of anonymity on the internet in the future[56].

In another attempt to gain greater control over the virtual space, Iranian authorities have also begun providing economic incentives for startups or developers to move their websites and services to servers inside the country.

For example, ICT Minister Mahmood Vaezi said that "his ministry is very keen to support Iranian developers to create mobile apps and other services by offering free bandwidth to Iranians startups"[57]. Nevertheless, it is difficult to estimate the percentage of Iranian services and websites which are currently hosted inside Iran. A Small Media report remarks that "the only official statistic shows that %34 of Iranian-owned website are hosted inside the country"[58].

56 Small Media (2014 /12), Ibid., p.3
57 Small Media (2014 /12), Ibid., p.3
58 Small Media (2014 /12), Ibid., p.3

# IRAN'S CIVIL SOCIETY - A DIGITAL PERSPECTIVE

## Introduction - Civic Activism & Digital Communication

Broadly speaking, the civil activist space has become severely limited and dangerous since the disputed 2009 elections and the subsequent crack-down of the so called 'Green Movement'. Surveillance, arrests and harsh sentencing of civil activists has been stepped up dramatically to intimidate people and prevent a repeat of the popular uprising that almost uprooted the Iranian regime for the first time since 1979. The authorities have learned from this experience and attempt to suppress any regime critical activities or anything that could be interpreted as not being in line with the regime perspective, by using a combination of fear, surveillance and punishment. An example for this is the death on of Iranian pop singer Morteza Pashaei whose funeral caused the largest crowd gatherings (16-14th November 2014) in Iran since the 2009 elections as the New York Times reported.[59]

The pop singer was widely popular in Iran despite that fact that many of his songs were considered "too romantic"
by the authorities to be played on state television. When the news of the passing of the -30year old Pashaei, after his struggle with cancer, travelled around popular social media networks, instantaneous crowds started forming all over the country to mourn his passing.

The NY Times reported that

> police officers in riot gear closed the gates to Tehran's sprawling Behesht-e Zahra cemetery after thousands of young people flooded the site, singing Mr. Pashaei's songs, but also using the occasion as a rare opportunity to flirt and enjoy the excitement of a crowd.[60]

As a result of the greater risks and more hostile environment, civic activism has gone 'underground'. Instead of holding public events, hanging up posters, printing leaflets, joining demonstrations, much of the activism now happens predominantly online - utilizing social media platforms, websites, email distribution lists, blogs, and conferencing software such as gotoMeeting or Skype. Given the increased threat, activists have also become more careful with disclosing their identity online or doing any kind of traceable work. One one hand, this has led to more individual security but on the other hand it has let to less transparency as people are often unsure with whom they are communicating in their networks.

The widespread increase of social media campaigns and rapidly growing digital activist space has also revealed another conundrum.

59 Thomas Erdbrink (2014), New York Times, Public Grieving for Pop Singers Is Startling Iran, http://www.nytimes.com/17/11/2014/world/public-grieving-for-pop-singer-is-startling-for-iran.html

60 Thomas Erdbrink (2014), Ibid.

Since the offline campaign work was forced 'underground' to the realm of the arguably safer online realm, many of the more seasoned (pre2009-) activists feel that post2009- digital activists have become a little bit "delusional" in believing that everything can be done and solved with online tools. They do not question the undisputed opportunities the digital world offers but argue for a more balanced approach that combines both online tools with offline efforts. In an interview, one woman's health/rights activist stated:

> During the years following the 2009 elections we have been practically at home and the constant usage of internet made us delusional. We thought we are revolting with Facebook but marginalized areas stayed forgotten. It is better now. We are travelling; we are in contact with women. And we are also spreading information with the aid of Facebook, and group emails.

Another interviewee said:

> The big problem that has occurred is that we turned into internet-only activists. We write statements, sign petitions and start campaigns on the internet without considering that our audiences are restricted to only ourselves. That is the problem of civic society in Iran. Because of the restrictions to our freedom we are not able to work effectively, and so we revert back to organize online campaigns only.

Despite this critical perspective, digital activism and campaigns are crucial to keep the activist spirit in Iran alive and growing since it is the only "safe" way to continue this type of work. Successful digital campaigns can have a huge impact and are able to galvanise people around a cause. At the very least, awareness and social action are raised, but at best, successful campaigns can bring an otherwise neglected topic to the forefront of worldwide media attention. One such example is the Stealthy Freedom campaign which started as a Facebook group that encouraged Iranian woman to post photos of themselves without their hijab or headscarf. The Facebook group was created on 3rd May 2014 and within two weeks had gained 170.000 followers. At the end of 2014, the group had 750.000 followers and received media coverage around the world. Another example were the protests in Isfahan in October 2014 against acid attacks on Iranian woman by religious hardliners who feel that their targets don't dress appropriately. After news of several such attacks, which have claimed one life so far, have been shared via social media networks, Isfahnian citizens took the streets to demand authorities to bring an end to these vicious attacks which have sparked so much outrage.[61]

There's no question that the security of Iranians is compromised. To improve it however, one must first analyse how security is defined.

61 The Guardinan (2014), Iranians protest over acid attacks against women, http://www.theguardian.com/world/2014/oct/22/isfahanisprotest-over-iran-acid-attacks

It is suggested here that, in order to elevate the security of Iranian activists, an integrated approach to individual security is needed. This approach consists of three overlapping spheres of individual security that affect one each other. Only by addressing and improving all three spheres, can the overall security of Iranian activists be truly changed for the better. The first sphere is called Psycho-Social Security and it relates to our perceived sense of security. As the threat awareness in Iran is high, it automatically and often subconsciously affects the emotional well-being of everyone living and working under these conditions. Finding the means to reduce this burden and thus improving the psycho-social security of activists in Iran must be part of the overall solution. Physical Security, the second sphere, is equally important as threats to people's physical well-being (jail, harassment by authorities or even the death penalty) are an ever-present and well known possibility for Iranian activists. As such, tools and means need to be found and deployed to increase the physical security of activists in Iran. Last but not least, is the strong need for Digital Security which affects the security of activist's information & equipment and by extension also that of their physical and psycho-social security. Given that the majority of activism in Iran happens online, the need for digital security is bigger than ever. Therefore, a holistic sense of security for activists in Iran is only achieved if all three security spheres are appropriately addressed. To achieve this, it helps to understand that there has also always been a close link between the role of information in physical threats to digital activists and techniques for psychological intimidation and control. In this sense, many of the threats emerging in the digital age that seem new are simply extensions and expansions of wellestablished practices for the control and curtailment of freedom of expression, association and assembly. Understanding this history is important as it can help digital activists to not only concentrate on the unique and complex technological challenges of the present but instead learn from the responses of the past.

# Civil Activism and Digital Communication!

This also helps activists to recognize which threats are established practices, which have been extended into the digital sphere and which ones are new.[62]

One of the primary issues for digital activists is that digital technologies become part of their regular working practices (e.g. social media). However, the paradox is that as technologies become easier to use, they also become increasingly more difficult to control, thus reducing the number of endusers with the expertise to understand how they work, where information is stored, what data is collected, and who has access to it.[63] This can be very dangerous and problematic as activists increasingly rely on mainstream tools because of their ease to use and broach reach. But at the same time, mainstream tools can also easily be abused to become 'honey-pots' for those who wish to entrap activists. Moreover, the lack of transparency and data control might be negligible for an average user but for a digital activists or high-risk user this can be very dangerous and problematic.

In the words of Hankley & Ó Clunaigh:

> … given the resource differential between HRDs (Human Rights Defenders) and many of their adversaries and the rapidly developing technological climate, the community of practitioners trying to build HRDs' capacities in digital security can no longer afford to adopt an approach that fosters dependence upon their direct advice in order to stay safe. Although it represents something of a mammoth task, a coherent and holistic approach to HRDs' security must go beyond any one approach. It must foster critical thinking, be fully informed by shifting needs and practices emerging from the field, and must be addressed within the overall question of how to protect and enable the work of HRDs.[64]

## Coping with Digital Insecurity - A Needs Assessment

To determine the value of the digital space for civil society in Iran, the authors of this report conducted a targeted study with civil society actors consisting of surveys and remote and in person interviews of activists living in Iran and working in varying fields such, environment, education or human rights. They were asked a series of questions to gain further insights about how the digital situation in Iran is restricting their work as well as about what opportunities and potential the digital space offers them. The resulting answers and analysis are the backbone for the following needs assessment report and the foundation for the recommendations this report will be providing.

All interviewed activists defined the internet or digital space as extremely important and useful for their work. Predominantly, they rely on the digital space as a source of knowledge and information, such as awareness about current events or global

62 S. Hankley & D. Ó Clunaigh (2013), Ibid, p. 537
63 S. Hankley & D. Ó Clunaigh (2013), Ibid, p. 538
64 S. Hankley & D. Ó Clunaigh (2013), Ibid, p. 5468

campaigns, scientific research and knowhow for their respective fields of work. An overwhelming majority stated that almost all their campaign and professional resources, such as books, magazines and manuals, are obtained via the internet and then translated from English to Farsi as this type of activist knowledge is hardly available in Iran itself. Equally, many activists stated that they and most young and middle-aged Iranians do not trust the state sponsored media outlets and rely on the internet as a medium for independent inquiry. The digital space is also the best way to recruit new members or find campaign supporters according to the interviewees. Last but not least, the digital space has been defined as an invaluable asset for documenting and raising real-time awareness about human rights violations. This gained awareness or forced transparency makes it much more difficult for authorities to cover up regime-sponsored crimes against Iranian citizens and is an important mechanism to bring information to the attention of the international community and as such at least slow down the authorities in their endeavours to crack down on civic society actors. In the best of cases, human right violations can reach world wide attention and result in international diplomatic pressure on Iran.

However, as mentioned in the previous section and given the government crackdown and increased pressure on civil activists, there is some disappointment that activism is now largely limited to the virtual space. Online campaigns, blog posts, twitter campaigns and facebook groups have popped up all over the place and become the weapons of choice for a disenfranchised group of activists and everyday citizens. The survey conducted revealed that 93% of all activist respondents spend between 5-3 hours per day in social networks. This is almost twice as much as the average American user.[65] The questions has thus become how effective these online tools are and whether Iranian activists are equipped to make the most of these tools without endangering their security. One interviewee stated:

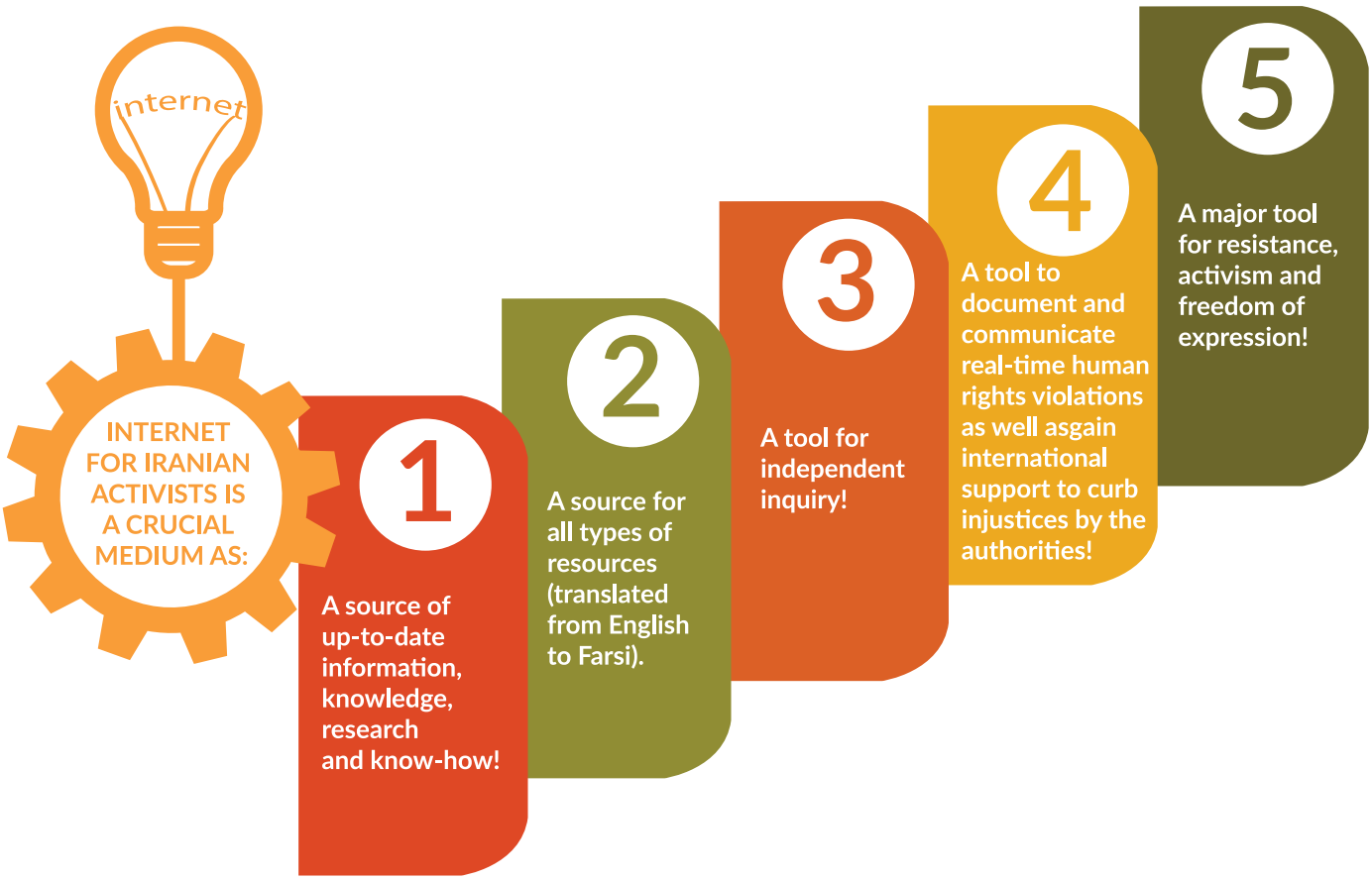
> Many activists just see the influence of their work in quantity of their “likes” or page views and do not try to go beyond it (into reality). They are satisfied by “likes” and they think they are doing a serious job.

This critical assessment of online activism raises a very valid point - namely that of understanding digital campaigns. What can they achieve, what can they not achieve as well as how does one define and measure their success? It is true that many Facebook groups won’t bring about the desired change or even a regime change but to condemn them as pointless and ineffective would be equally misguided. They should be viewed for what the are - microcosms of resistance and places for freedom of opinion and online expression. Nevertheless, it is also true that these online forms of resistance have the potential to be much more than that.

65 AdWeek (%28 ,(2015 of Time Spent Online is Social Networking, http://www.adweek.com/socialtimes/time-spent-online/613474

As such, it is upon digital activists to equip themselves with the knowledge and know-how to make the most of the online tools at their disposal whilst taking great caution not to endanger their own or other people's digital and physical security. Unfortunately, the survey has also revealed that this is not yet the case as digital activists seem to lack a basic understanding of how to act responsibly within social media networks. An example of this is the fact that 96%of respondents use Facebook but only58% restrict their profiles and generated content to a closed circle of friends and trusted contacts and 42% openly share their information with the public. This clearly demonstrates that there is a great need for educating digital activists about social media, how to use it effectively, as well as how to use it responsibly without compromising anyone's security.

**KEY TAKEAWAYS - THE INTERNET FOR IRANIAN ACTIVISTS IS A CRUCIAL MEDIUM AS:**




Every interview participant stated that the digital restrictions in Iran or fear of being surveilled were their primary concerns. This is evidenced by the fact that out of 100 respondents %92 did not want this report to use the name of their organization(1% answered "yes and 7% answered "n/a"). The only noticeable difference was between those activists that worked in fields relevant to the political situation in Iran and those that didn't. For example, environmental activists who are organizing campaigns to clean up parks in Tehran did not fear government surveillance because they believe their work is not anything the authorities would object to.

However, even those activists are frustrated by the existing digital restrictions - most of all the slow internet speeds and the blocked websites and social media platforms which impede their efforts to run effective campaigns, form new networks or simply create more awareness about their causes.

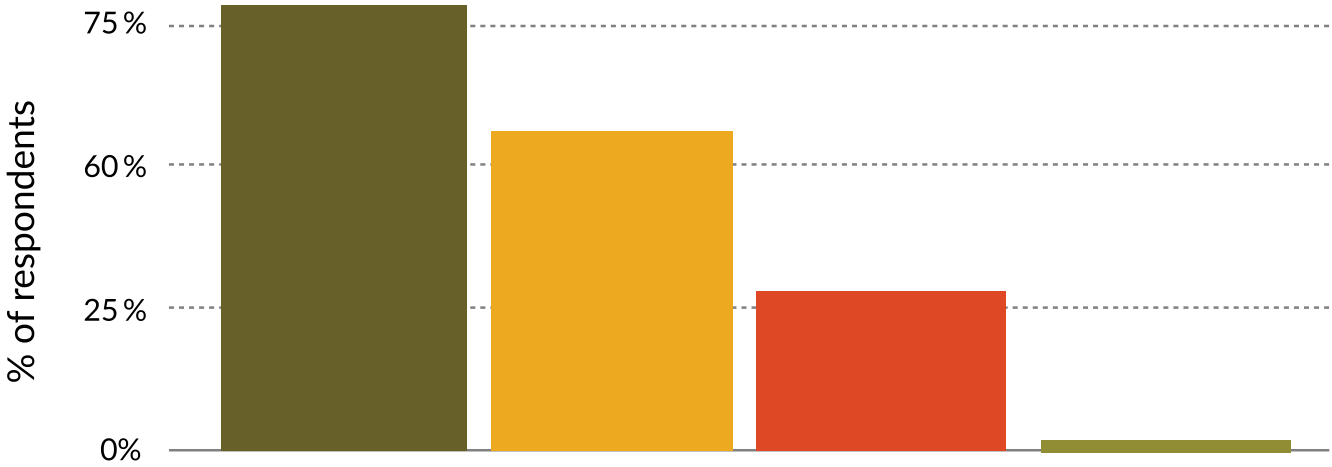
The primary concern, however, affecting everyone equally are the severely reduced internet speeds which make it difficult from Iranians to obtain resources such as larger PDF documents (e.g. reports, books & magazines), video documentaries or useful software solutions. When asked to rate their challenge of slow internet %91 of respondents felt either “challenged” or “strongly challenged” and 8% “moderately challenged”. Another concern for digital activists is the filtered content and the fact that many useful websites and social media platforms are blocked and are only accessible through VPNs (virtual private networks) or proxy servers (which often further slow down internet speeds and require a decent background of ICT knowledge). In the words of one of the interviewees,

> Coherent civic activities cannot be expected when there is no access to information. This is the age of digital and virtual communication. We cannot expect to stick a poster on the wall and want people to attend an event. Internet disconnection, low internet speed and filtering really hurt our activities.

This is evidenced by the fact that 77% of respondents felt “challenged” or “strongly challenged” and 20% “moderately challenged” meaning that only 3% of respondents had little to no challenge with internet filtering.

The third concern, which is not only affecting those activists that are working in the human rights space, but also anyone who engages in any type of political or religious expression, is the fear of arrest and punishment brought about by digital surveillance. It would be a mistake to minimize this concern because it hinders civil movements from growing and also silences and stops a majority of those that would like to speak out or take action - all because of an environment of fear. As exemplified in the previous chapter, this fear is based on more than enough cases of arrests and severe punishments to the point where it has become an ever-present concern for anyone communicating online or by phone.

Moreover, despite the fact that ICT knowledge of Iranian activists is higher than that of the average citizen, and the fact that a general awareness about government surveillance exist, another concern stated by the interviewees is that most people active in the digital space simply do not have an adequate knowledge about how to protect themselves when using online or voice communication. Interviewees stated, for example, that many people keep using Viber, WhatsApp or Skype to communicate sensitive information, which could get



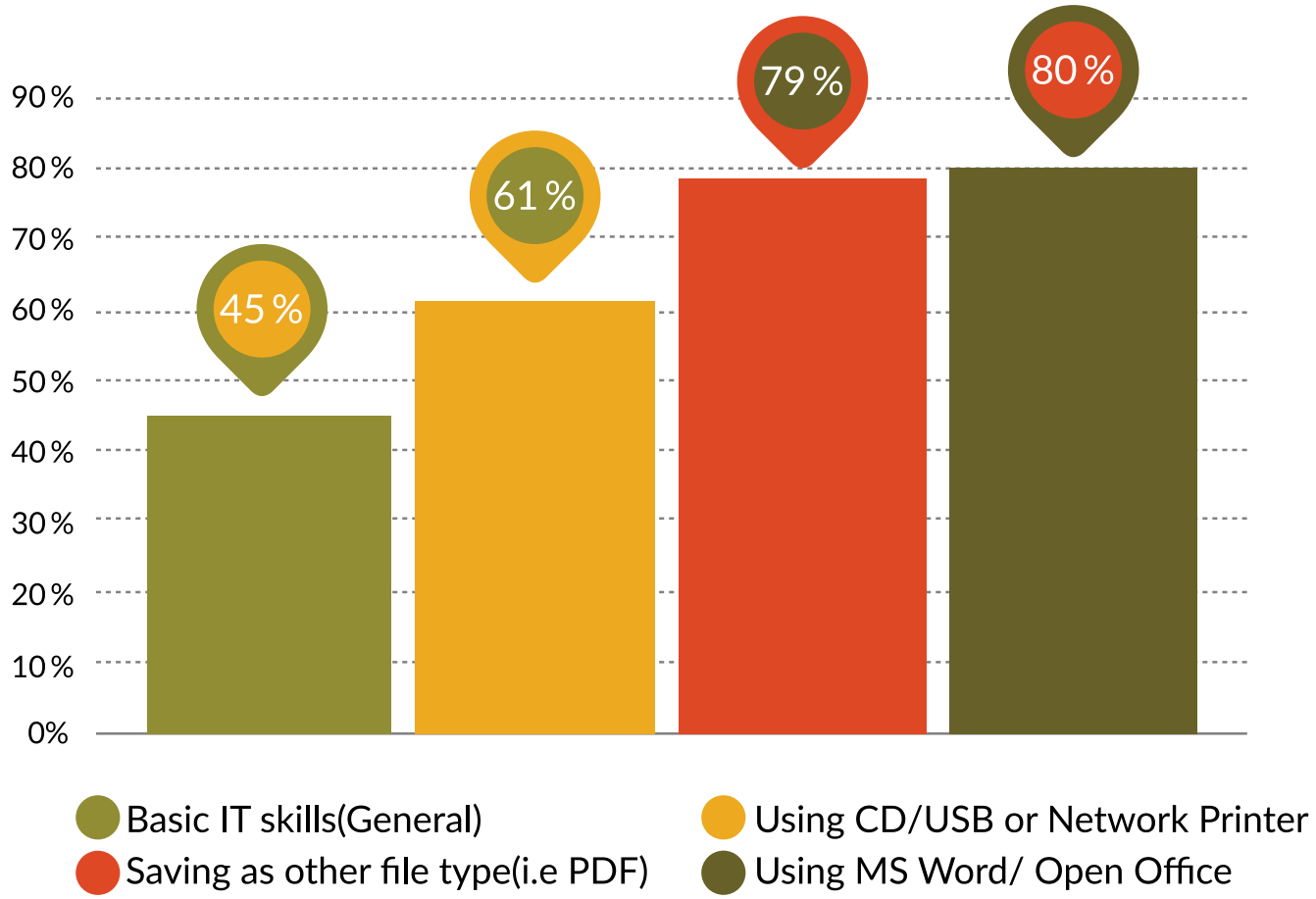

them and their networks into trouble if such messages were intercepted by the authorities, because people do not know about alternative and more secure means of communicating. In fact, often people do not even use two-step verification for their Gmail accounts which is the most basic form of account protection.
The fact that most Iranian activists possess an awareness for the existing threat and have a basic rudimentary understanding of online security, does not mean they are acting in a safe manner. This is evidenced by an overwhelming majority of 85% which rate the likelihood that they have been hacked or subjected to a cyber attack as "strong" or "good". Nevertheless, the survey revealed that only 59% feel they are using a "strong" or "good" password for their computers.

Similarly, when asked about using password management tools (ie. LastPass) , the survey discovered that only 45% rate their ability to use such tools as "strong" or "good". This indicates that the remaining 55% don't use such tools from which one could deduct that they are either using easy-to-remember passwords (not safe) for their various accounts or repeatedly use the same strong password for several sites (also not safe). Moreover, only 44% rate their ability to identify dangerous emails or URLs as "strong" or "good" and only 38% rate their skills with anonymous software like Tor and Freegate as "strong" or "good".
The survey also highlights that only 8% of respondents are likely to protect their Excel sheets with a password. The apparent contrast between threat awareness and inability to take appropriate measures to reduce the threat can only be explained by a lack of training and knowledge.

In order to to understand the causes for the above mentioned inconsistency, the survey also asked about the basic IT knowledge of respondents which revealed that between 41%-49% of activists still rate their basic IT skills either "weak, not good or average" . The more complex the task gets the bigger the drop in respondents that feel confident about their skills. For instance, when asked about their ability to use software that is dependent on CD-Drives or USB Flash drives or using a shared resources on a

network (eg. shared printer), the number that rated their ability as either “weak, not good or average” increased to 60%-61%. When asked about their ability to search for and find a file on their computer or use and connect external devices such as printers, scanners or projectors - the number of participants that felt either “weak, not good or average” further increased to 80%. Also when asked about using basic office software like MS Word or Open Office and performing simple tasks, 80% of respondents rated their ability as either “weak, not good or average” The same is true for 79% when asked about their ability to save files in other formats such as PDF. This is clearly a big concern as one cannot expect. Moreover, only 2% of respondents stated that they feel no or little challenge by lacking ICT skills. The overall majority however responded that they usually experience challenges in their work due to missing ICT know-how (32% “moderately challenged”, 44% “challenged” and 20% “strongly challenged”).

**Respondents rating their IT abilities as eaither “weak”, “not good” or “average”**

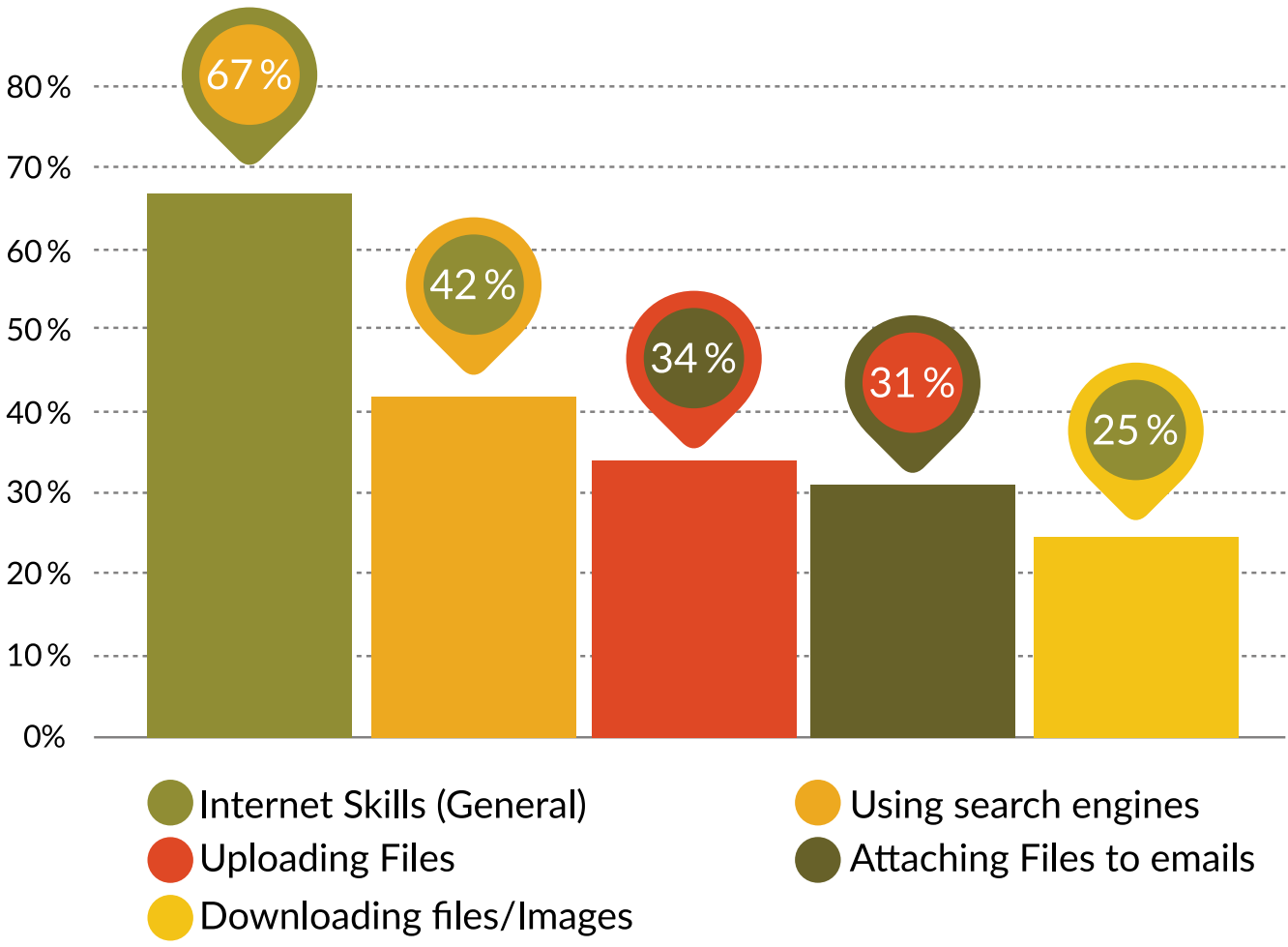


Another concern is the fact that many people - especially in rural areas - do not even have access to the digital space because computers and bandwidth are expensive. This often only allows them access via internet cafés which - as argued in the previous chapter - are not secure at all. Also the lack of software is a key issue of digital activists. 66% of survey respondents stated they they felt "challenged" or "strongly" challenged and 24% "moderately challenged" by the lack of access to software.

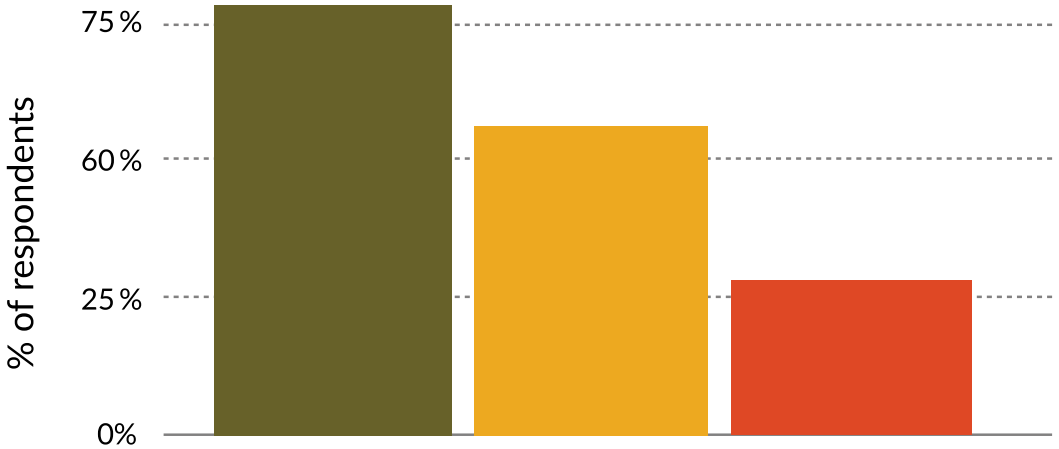
The lack of access to the digital space as well as to specialized software also results in the accompanying lack of digital know-how. This is especially true for rural areas. One interviewee stated for example:

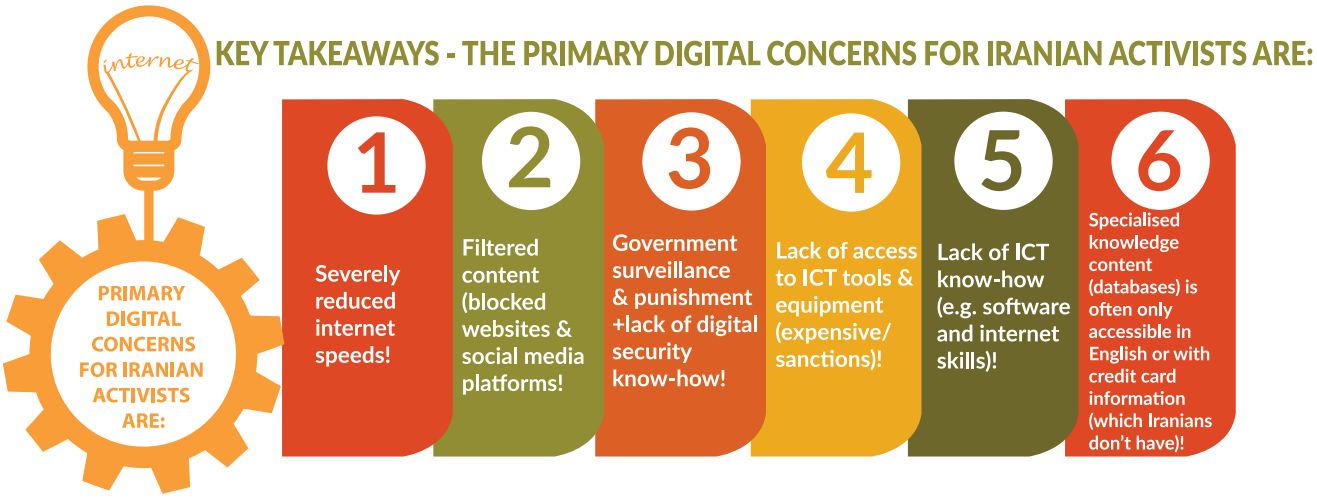
> Unfortunately many of our colleagues and friends do no even know how to attach a file when sending an email. There has been not enough work in small cities to educate people. Activists need education. Unfortunately, the internet is still a luxury and not an everyday tool in many places.

**Respondents rating their internet abilities as eaither "good" or "strong"**

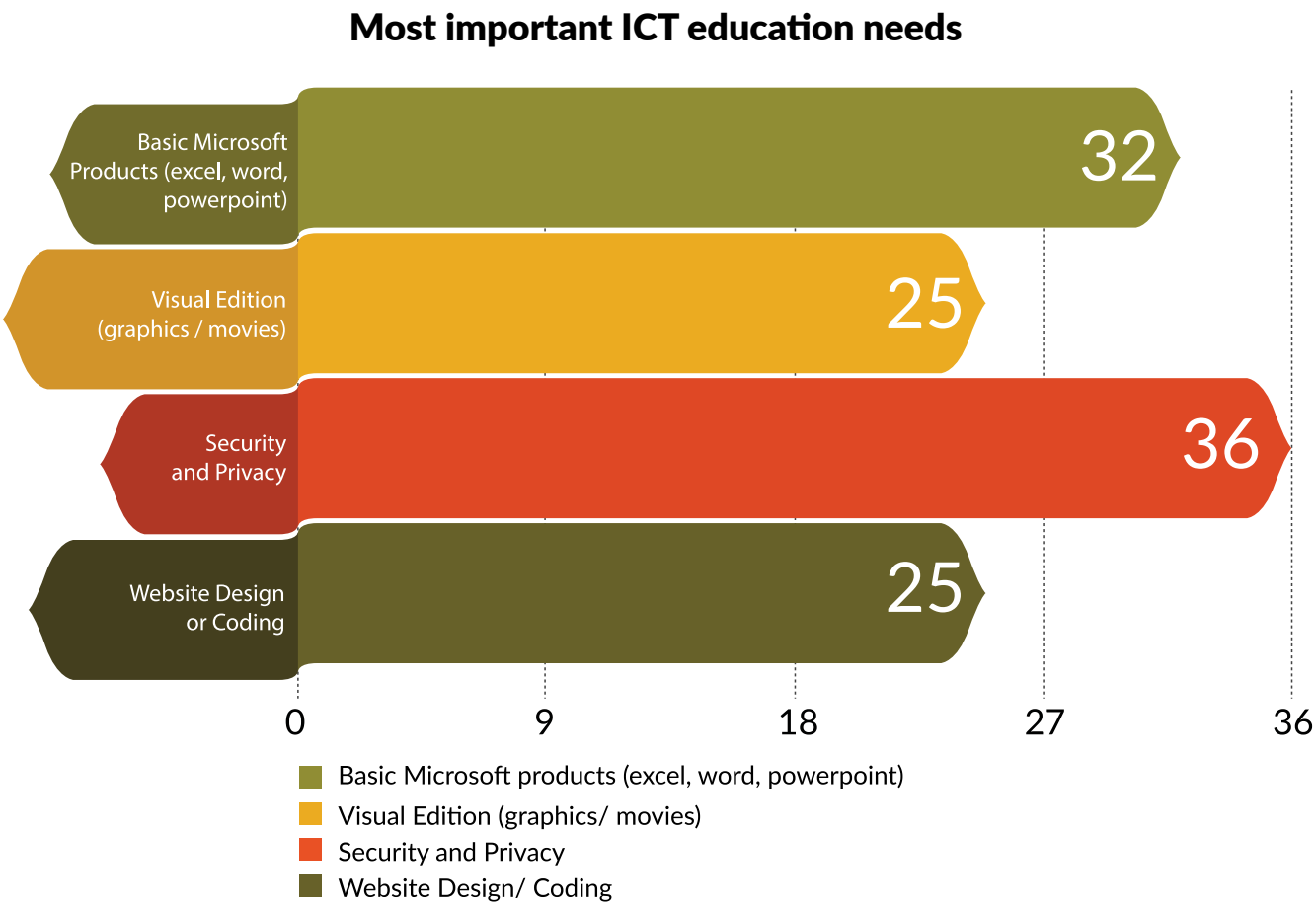


The survey revealed that 67% of respondents rated their ability as either "good or strong" when asked about how comfortable they felt using the internet in general. As soon as the task got more specific, the comfort level of respondents rating their ability as "good or strong" began to drop to 42% (for using search engines), 34% (for uploading files), 31% (for attaching files to emails) and 25% (for downloading files and images from the internet). These figures clearly highlight that there's a huge knowledge gap in basic IT training. Naturally, a basic ICT education is required before anyone could even begin to understand the means and tools to protect themselves when using online or voice communication. This is a strong need and the minimum starting point before teaching more advanced software or online security skills. Also the use of online courses could be a strong tool to share knowledge and knowhow about ICTs in general or even pass on knowledge about basic online security. When asked about this possibility, many interviewees stated that they would find such online courses useful. However, a little more than 50% of all interviewees have not participated in such courses yet - also because they find them not always relevant for an Iranian context but also impractical for Iranian time zones (e.g. evenings when internet cafes are closed) and sometimes not even accessible because of US sanctions (e.g. Coursera). Another concern this report would like to highlight is the fact that a few interviewees have expressed an issue with accessing high quality specialist knowledge-content (e.g. academic journals or medical research papers). The experience they've had is that many of such database portals, where one could acquire such knowledge-content, were either closed to non-members or only available via payment with credit card information which Iranians don't have since both VISA and Mastercard are US based and therefore not available for Iranian citizens (due to decades of international sanctions and embargoes). In addition, the majority of such content is only available in English and first has to be translated into Farsi to become useful. Once again the survey evidences this point as 87% of respondents stated that they are "challenged" or "strongly challenged" by not having access to knowledge databases. 11% felt "moderately challenged" by this fact.

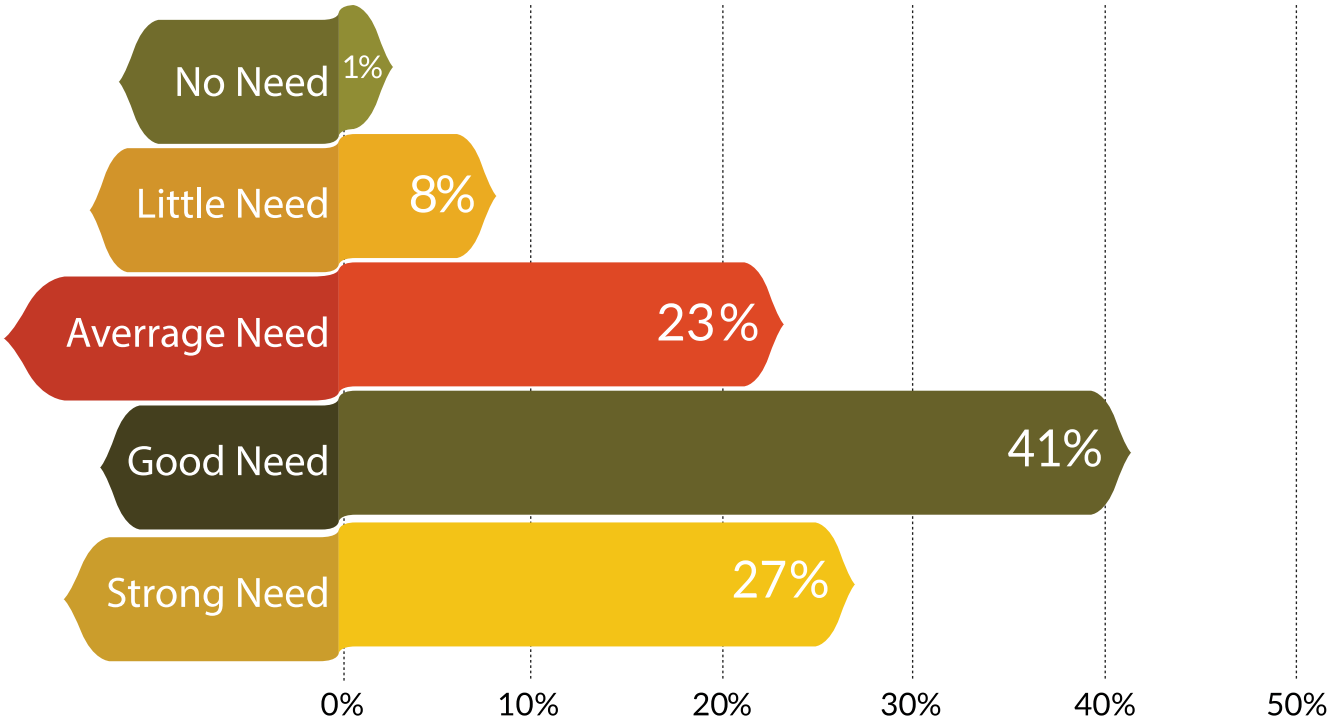




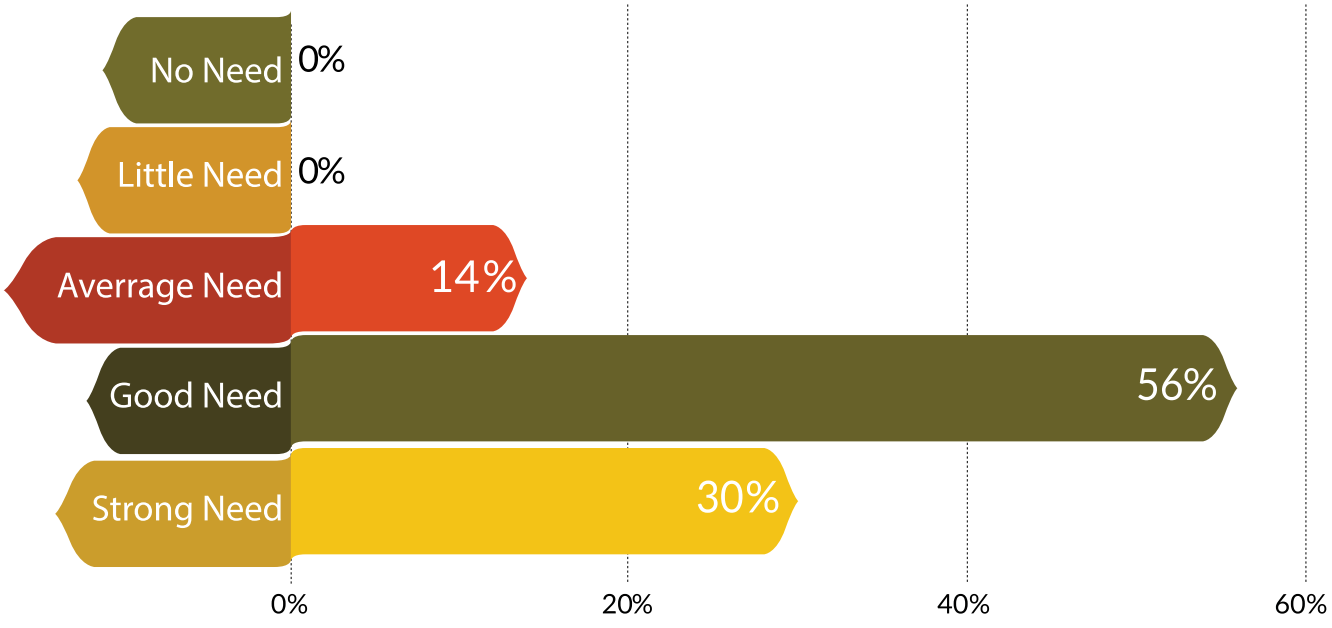

Nevertheless, the survey has also demonstrated that Iranian activists have a great willingness to expand their knowledge and skills, optimize their social media campaigns and increasingly use rich media (graphic, video and audio) content to further the goals of their work or organization. They are acutely aware of the need for more ICT education - whether it is training related to software, security, social media or coding. When asked to define their most important education needs, the survey revealed the following:



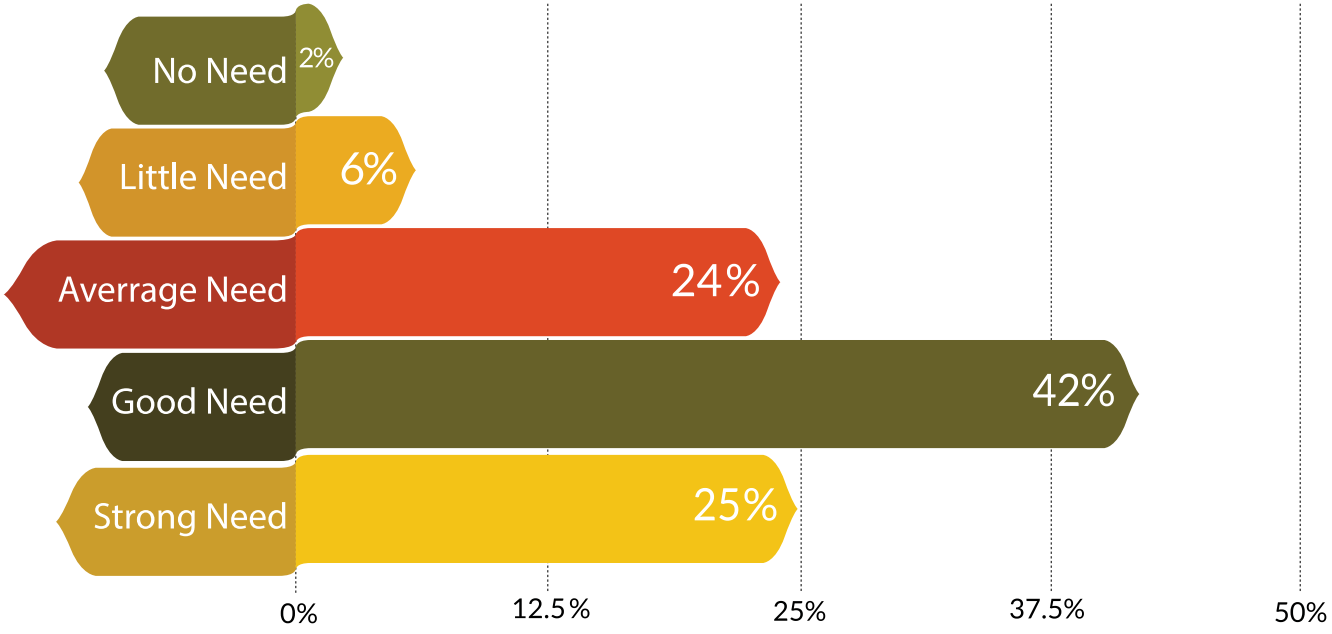
A more detailed breakdown of educational needs for digital activists can be found below.
Need for elementary ICT education (e.g. working with Word, Excel, PowerPoint, Email sign up & management, online digital archiving, etc).



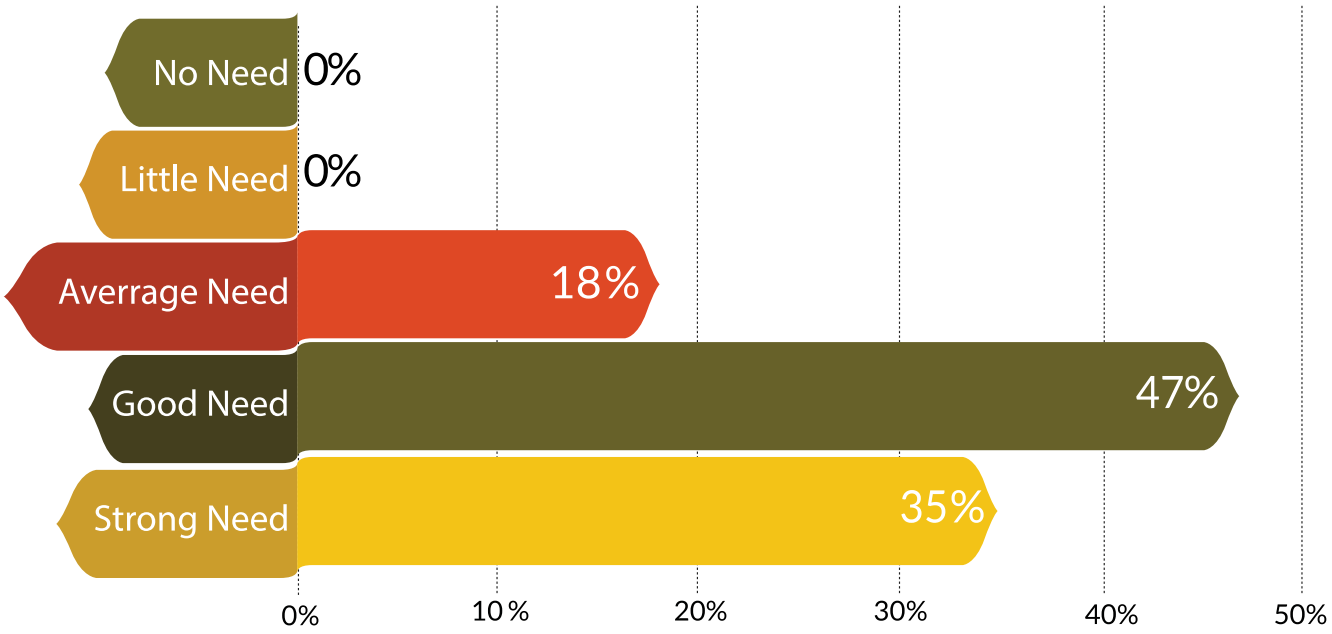

Need for professional ICT education (e.g. working with project management software, Excel, PowerPoint, CRM software, etc).



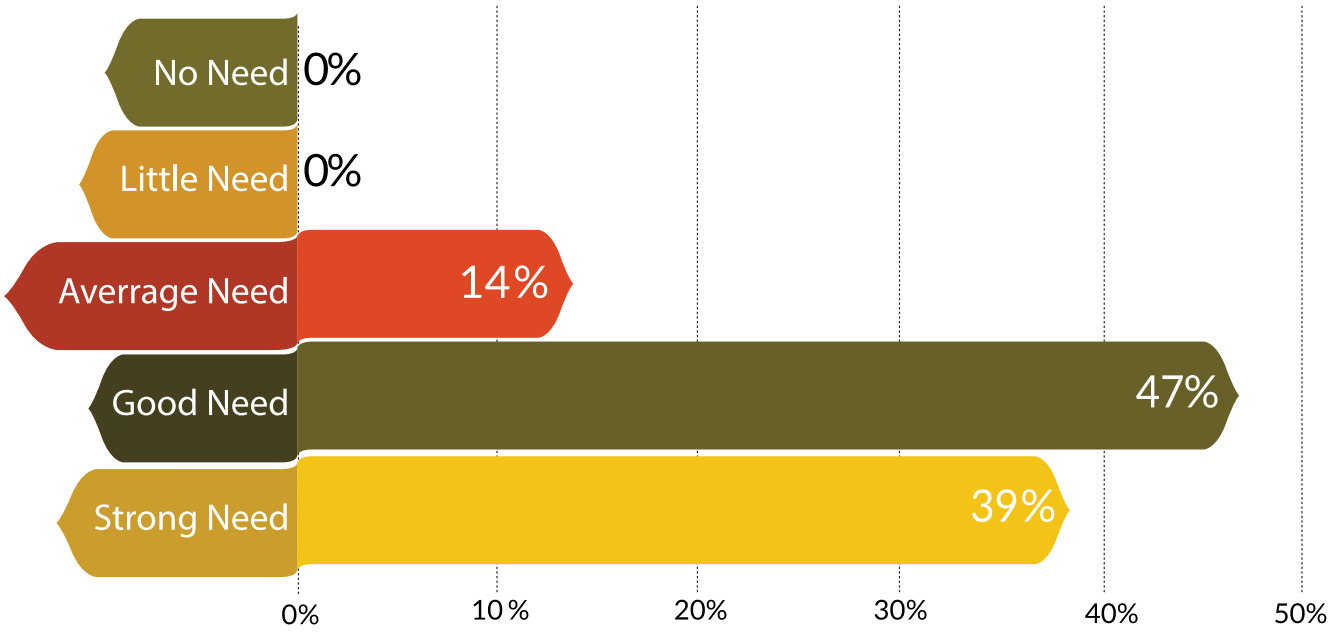
**Need for basic online security while using the internet**




**Need for security & network education (advanced)**

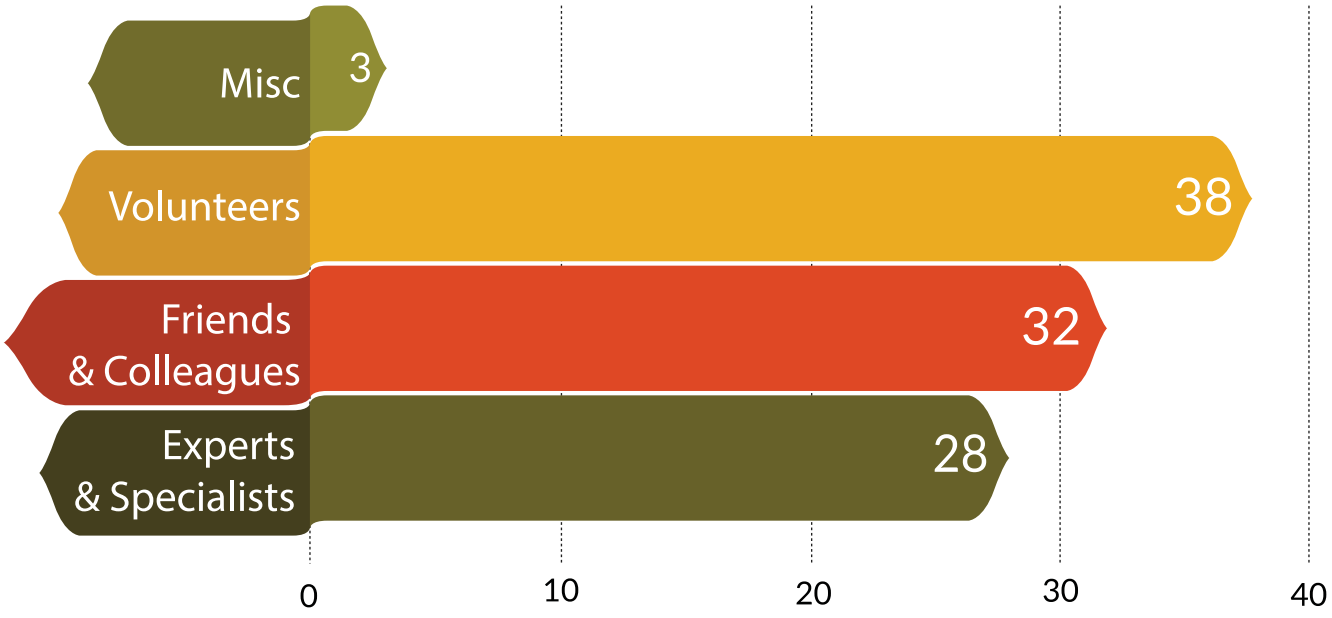


**Need for education about social networks, expansion & advocacy**




The survey also highlighted a strong need for access to professional ICT experts or specialists as the majority of activists consult only colleagues or friends when faced with crucial ICT or computer issues.

**Who helps you in crucial situations with ICT or other computer issues?**



In summary, the following catalogue provides an overview over the issues and needs identified by Iranian activists and organizations.

| Key Issues / Needs | Activists & Organizations | Public |
|---|---|---|
| Lack of basic ICT skills / basic ICT training! | X | X |
| Lack of advanced ICT skills / advanced ICT training! | X | |
| Lack of access to specialized software and software training! | X | |
| Constant fear of cyber attacks, arrest and detention due to surveillance of Iran's cyber army. Need: Training about basic digital security practices incl. access to tools and apps | X | X |
| Lack of ICT counseling centers, capacity building organizations or professional support for general ICT questions or specific ICT security training. Mentorship / Training of Trainers program! | X | |
| Filtered content (lack of access to information) as well as lack of trusted and available VPN's | X | X |
| Low internet speeds / Low-weight information and software! | X | X |
| Restricted access to expert-knowledge databases or online training courses! | X | |
| Lack of access to information in Farsi! | X | X |

## RECOMMENDATIONS:
## MEANS AND TOOLS TO SUPPORT DIGITAL ACTIVISTS IN IRAN

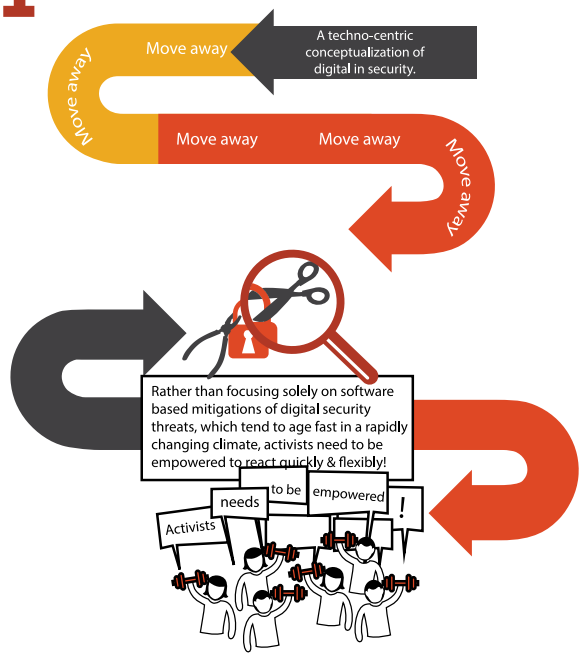
After analysing both the digital landscape in Iran as well as providing a first hand needs assessment of Iranian digital activists, this report would now like to propose a number of recommendations which are based on the insights obtained above. These recommendations serve the purpose of identifying the means and tools to support digital activism in Iran and helping activists to better protect themselves from persecution or simply to increase their awareness about digital security in general. As Hankley & Ó Clunaigh describe it;

> In this regard, significant progress has been made over the past decade in the field of digital security … However, there is much work that remains to be done. It is extremely hard for those working in different ways to keep up with the diverse range of fast-changing threats. The demand for such support often outstrips the level of response available, and shortcomings in the responses to what has become an extremely complex terrain are increasingly being identified. In particular, each of these approaches could greatly benefit from more information sharing and coordination.[66]

66 S. Hankley & D. Ó Clunaigh (2013), Ibid, p. 540

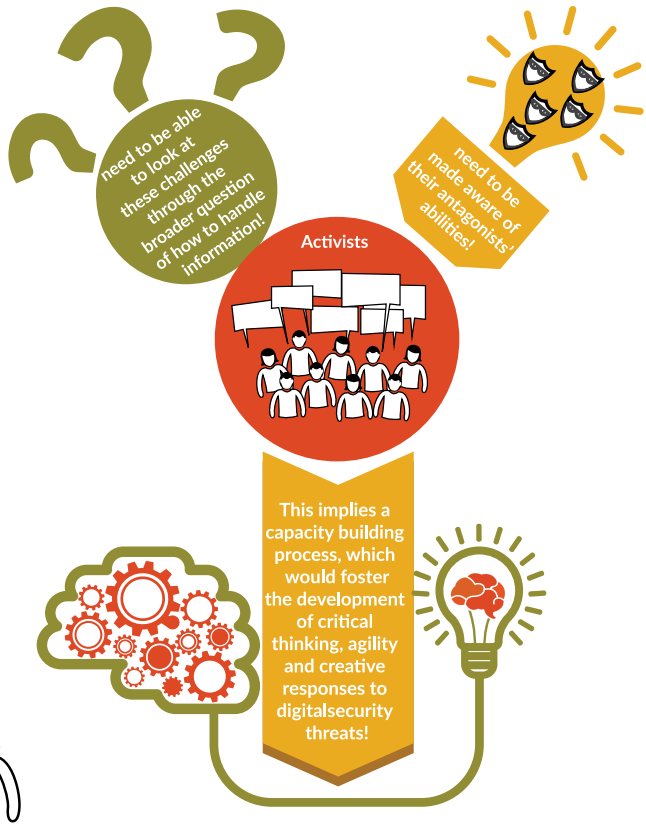
The final report recommendations are also guided by the following suggested overall principles derived by Hankley & Ó Clunaigh (2013). These are:

1



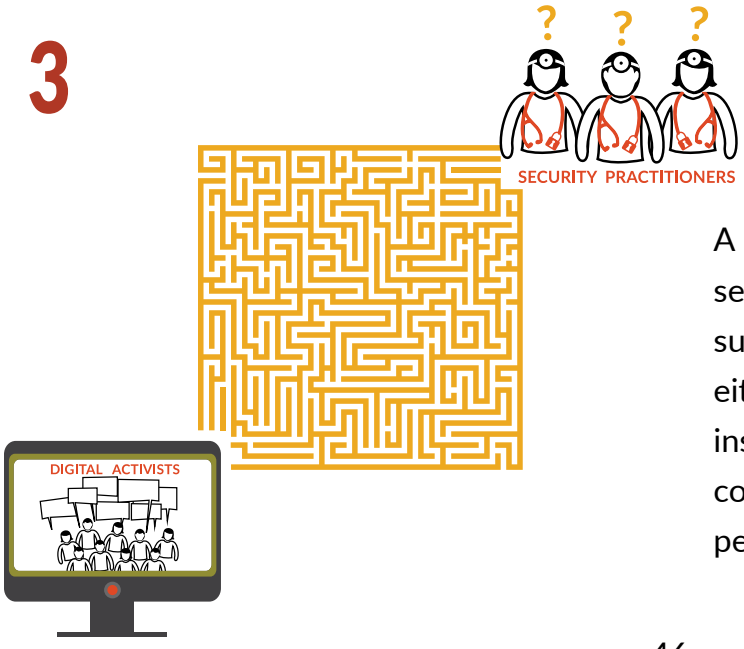

A need to move away from a techno-centric conceptualization of digital (in) security. Rather than focusing solely on software-based mitigations of digital security threats, which tend to age fast in a rapidly changing climate, activists need to be empowered to react quickly and flexibly.

2



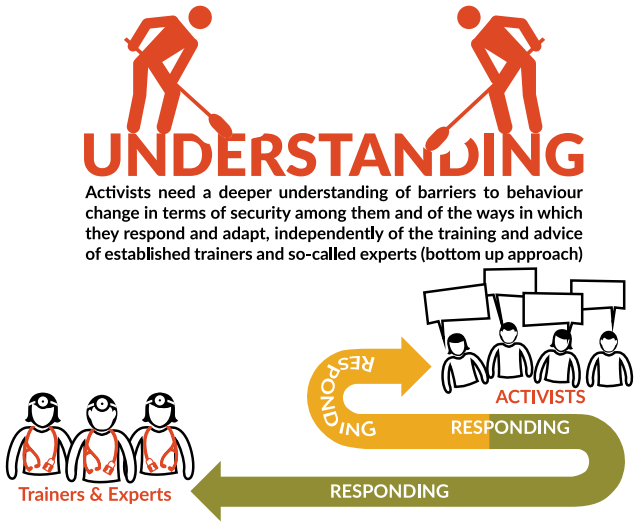

Activists need to be made aware of their antagonists' abilities but also need to be able to look at these challenges through the broader question of how the handle information. This implies a capacity building process, which would foster the development of critical thinking, agility and creative responses to digital security threats.

3




A need on the part of some digital security practitioners who take a 'zero-sum' approach to digital security ('you are either completely secure or completely insecure') to recognize the inherent complexities of the context, work and personal lives of digital activists.

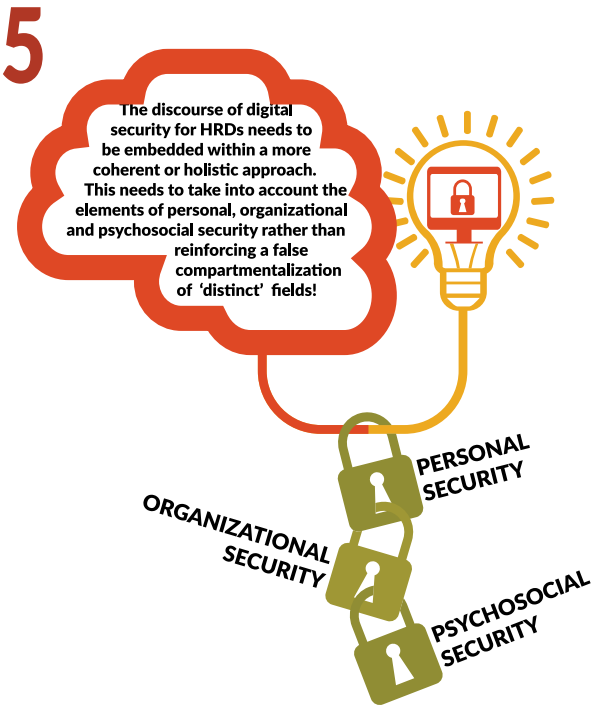
4




Activists need a deeper understanding of barriers to behaviour change in terms of security among them and of the ways in which they respond and adapt, independently of the training and advice of established trainers and so-called experts (bottom up approach)

5

The discourse of digital security for HRDs needs to be embedded within a more coherent or holistic approach. This needs to take into account the elements of personal, organizational and psychosocial security rather than reinforcing a false compartmentalization of ‘distinct’ fields.



REPORT RECOMMENDATIONS / TOOLKIT

A) IRANIAN CIVIC ACTORS & ORGANIZATIONS

Information that is directly released to activists and also hosted on password protected and secure networks.

A1) Security (Technology Based Solutions)

USB based Operating Systems

Given the high risk of being caught with incriminating evidence, we propose to distribute and make available USB based Operating Systems which can be unplugged and destroyed at a moments notice. This would dramatically increase the security for people dealing with sensitive data.

Reliable and Secure VPNs

We can also offer to set up reliable and secure VPNs on either a batch order or ad-hoc needs basis to enable civic actors to circumvent the Iran-based filtering procedures. This would allow them to access resources they would otherwise not be able to study and use.

Penetration / stress test on websites and free security consultation

Digital starter kit containing apps and tutorials

The purpose of this kit would be to provide a list of secure everyday apps and software which will aid activists in their work whilst better protecting them from surveillance measures. The list would also provide download links for the apps and software (license free) as well as tutorials on how best to use each of them.

Cooperation with anti-malware vendors to offer free software with support for Iranian activists

A2) Training & Education (Capacity Building)

101 security toolkit detailing basic digital security practices

We propose the creation of a light-weight Iran-specific toolkit (downloadable and online) which details an introduction to web security and step-to-step guidance to basic digital practices to better protect users. The toolkit would be available in both English and Farsi and could be in form of a blog or a website which features both text and video introductions. Each topic and video could be downloadable as a lightweight version to better facilitate duplication amongst Iranian users.

Digital Coachings & Trainings + Mentorship Program

We'd also offer -1to1- coaching and trainings for organizations to improve their collective digital security practices. In addition, we'd offer much needed mentorship programs to enable and empower individuals to become digital security trainers themselves who will help to multiply the digital security benefits.

Introduction to social media & digital campaigns

This kit would consist of an introduction to and how-to-guide for the most popular social media platforms. The objective is to understand the strengths and weaknesses of each platform and what it can be used for. The kit would also include example of how successful online campaigns work and most importantly how success can be defined and measured.

Cloud database containing all necessary software, training, and secure operating system files

This database would be a growing repository of all the knowledge and training materials developed and collected.

Government Policy Updates

Monitoring policies and programs of government to keep up-to-date with attempts to restrict the flow of information between civil society activists and organizations

A3) Digital Support Platform and Rapid Response Team (Capacity Building)

Establishing a platform that allows civic actors to post questions / inquiries regarding technical issues. This would work like a online community where digital experts as well as the wider community would be collaborating to share knowledge and know-how.

Additionally the platform would offer an emergency hotline that allows users to get in touch with a team of digital experts that would respond to their inquiries. At times the response would be to simply direct users to a relevant thread in the community platform and in other cases it would mean a real-time engagement to assist the inquirer to get out of harms way or solve a critical problem / attack they are currently faced with. Examples could be one-on-one assistance when personal accounts like (Gmail, Facebook, etc.) have been hacked or they need help thwarting an attack on their organization, ensuring that they cleanse their system from any intruding elements (malware, keyloggers, viruses etc)

Further, the platform would post regular new updates on recent trends, thread and tools to keep the community up-to-date with the situation and alert them when new cyber vulnerabilities emerge.

B) IRANIAN PUBLIC (THESE ITEMS WOULD ALSO BE USEFUL FOR THE CIVIL SOCIETY ACTORS)

Information is hosted on publically available servers, including popular social networks and platforms accessible to all.

B1) Video tutorials and updates about digital security

This would include little video features aimed at a public audience to cover basic elements of digital security (e.g. why its better to use Telegram vs WhatsApp when one is concerned about privacy).

B2) Interactive FAQ Blog/Forum

This would entail a public platform which will host a series of FAQs about digital security. Additionally, users have the chance to send in questions or ask for advice.

# METHODOLOGY & BACKGROUND

Volunteer Activists
PEACE | DEMOCRACY | HUMAN RIGHTS

## Methodology

The report used quantitative as well as qualitative research methods and is the first quantitative and qualitative research conducted in Iran after an eight-year period of confinement and suppression of local activists. It focuses on the needs, challenges, capabilities, shortcomings and capacity of Iranian CSOs and social activists in the digital world. This research was conducted between November 2014 and February 2015.

Chapter one and two of this report (3.1 and 3.2 respectively) rely on secondary research - predominantly international studies and reports but also media reports. The third chapter (3.3) is predominantly based on first hand research through the targeted study conducted with CSOs and social activists in Iran.

The targeted study consisted of a questionnaire and in-person as well as remote semi-structured interviews of activists currently living in Iran. The study examines two areas that focus on the need assessment and capacity assessment of CSOs and social activists in Iran and addressed the following key questions:

1. In which areas do Iranian CSOs need support? Which gaps need filling in order to develop sustainable CSOs? These questions are founded on the present challenges facing Iranian CSOs in the digital world.

2. Which areas need most attention so that Iranian CSOs can maximize their organizational capacity and improve their performance? What are the unique capacity building needs of these CSOs and how can they be addressed?

### Research Methods and Data Collection

#### 1. Questionnaire

To have a better understanding of the needs and capacities of Iranian CSOs and activists in digital world, VA picked 250 organizations and activists based on their background, field of work and geographical distribution. VA then sent the questionnaire to each of these CSOs and activists via email. 170 CSOs and social activists responded.

#### 2. Semi-Structured Interviews

VA also conducted semi-structured interviews with 30 experts and civil society activists to gather insights and understanding of the needs and capacities of Iranian CSOs in the digital world. The participants, 12 women and 18 men, were selected on the grounds of their knowledge and experience, field of activity, gender and geographic distribution. 25 members of the group were managers and activists working for charities in the fields of health and hygiene, women rights and youth.

The remaining 5 members were university professors. The interviews were conducted based on semi-structured questionnaires with open questions. This allowed the interviewees to freely talk about the current situation of their CSO, their most important challenges, their impact on society, the most empowering reinforcements as well as any limiting restrictions, and future plans and strategies they had.

## Organizational Background

The research was carried out by Volunteer Activists, a non-profit organization that focuses on the promotion and expansion of democracy, the advancement of human rights and peace building in the Middle East with a particular focus on Iran.

The Volunteer Activists Institute is a non-profit, non-governmental, non-political and independent institute, the primary aim of which is

- capacity building among activists and civil society organizations;
- facilitation of information exchange among civil society activists,
- and advocacy and expansion of democracy, human rights and peace building within Iranian society in particular and communities in Middle-East in general.

The Volunteer Activists Institute designs and offers numerous human-centric capacity building programs to cater to the needs of civil society actors in the region. Furthermore their work facilitates effective knowledge and information exchange among civil society actors and organization; as well as supports networking opportunities for the actors in this space. They regularly publish research papers related to relevant topics in the effort to raise awareness and contribute to advancing the social discourse.

Address: Kabelweg 13, 1014 BA Amsterdam, the Netherlands

Telephone: +31 (0) 20 747 0195

Email: info@volunteeractivists.nl

Website: www.volunteeractivists.nl

Volunteer Activists
PEACE | DEMOCRACY | HUMAN RIGHTS