ARTICLE 19

Tightening the Net

Part 2: The Soft War and Cyber Tactics in Iran

2017

Executive Summary

"In this situation, we should know, before anything, what is happening in cyberspace so that we can use our knowledge, science, and persistence to defeat our enemy in the soft war."
Supreme Leader Ayatollah Khamenei

Despite being one of the region's leading cyberpowers, Iran is one of the worst violators of international standards relating to the Internet, routinely violating human rights exercised online, and using online tactics to restrict rights exercised offline. A regime-led ideological Soft War threatens to keep Iranian citizens isolated from the rest of the world, and unable to exercise their rights to freedom of expression and information. In order to understand how to address the challenges facing freedom of expression in Iran both off- and online, it is essential to understand how online control is implemented and maintained.

The Soft War has remained of great importance to the Iranian regime, with a particular surge in activity after the controversial 2009 elections, five months after which Supreme Leader Ayatollah Khamenei stated: "Today, the country's priority is to fight the enemy's soft war."[1]

There has been much discussion, by international civil society, as well as groups and individuals within Iran including members of the Iranian establishment itself, of an 'Iranian Cyber Army' (ICA) – an organised group with official oversight and support of the Iranian government. The origin and structure of this group are extremely difficult to establish, but there is clear evidence of online actors and tactics, whose actions and goals often align with those of the Iranian authorities, even shifting with that political agenda. Individuals and groups targeted by this group are often civil society, activists, and political opposition groups, though diasporic Iranians have also been targeted, as well as state entities seen as oppositional or a threat (potentially including the US Department of Justice[2]).

There are two distinct types of online activity which contribute to the hegemony of state ideology and discourse: the first is the content of the Soft War itself online – the production and promotion of state-sanctioned ideological content, with the restriction of content perceived to threaten tradition Iranian cultural and political values.

Those who express dissent, including social activists and human rights campaigners, (who frequently fail to adopt necessary online security precautions such as complex passwords and online anonymity) are monitored and even arrested. In subsequent interrogations they are often subjected to torture and other ill-treatment: the authorities thus obtain key information – communications, online account details, web histories – which enables the persecution of other targets of interest. This has been one of the most effective techniques in gathering information on human rights activists.

The second type of activity is cyberattacks i.e. hacking: intrusive malware, monitoring, and, for example, Distributed Denial of Service (DDoS) attacks carried out on actors perceived to be in opposition to state ideology: the targets are suspected of being selected by state actors, and civil society and political opponents have been shown to be primary targets of such intrusive tactics. This not only directly interferes with both the activities and publications of organisations deemed to oppose the government, but can also lead to information used to arrest and prosecute dissenting individuals or groups. It is important to note the difficulty in researching hacking actions and groups, especially in determining the attribution and intent of intrusive online actions.

Perhaps the greatest success of the Iranian government's online campaign, at least domestically, is the 'chilling effect': the establishment of a climate of fear that surpasses actual surveillance capabilities and encourages online communicators and activists to self-censor. It would be impossible to maintain a catch-all censorship or monitoring programme, but by instilling in Iranian citizens a sense of fear, the surveillance and blocking do not have to be comprehensive.

This report aims to provide an insight into the online tactics and networks active in Iran's Soft War, using a combination of primary sources, interviews, and metadata collection. (See Methodology)

[1] Supreme Leader Meeting with Basij Members, Khamenei.ir, November 2009, (online) Available at: http://farsi.khamenei.ir/news-content?id=8429 Accessed: 1 March 2016.

[2] Motherboard, US Charges Iranians With Coordinated Cyber Attacks on Banks, Companies, 24 March 2016, available at: https://motherboard.vice.com/read/us-charges-iranians-with-coordinated-cyber-attacks-on-banks-companies. Accessed: 1 March 2016.

Table of contents

Glossary and Abbreviations

Basij The Organisation for Mobilisation of the Oppressed (Basij) is a paramilitary volunteer militia established in 1979 by order of the Islamic Revolution's leader Ayatollah Khameini.

CCDOC Committee Charged with Determining Offensive Content

CCL Computer Crimes Law

CERT Computer Emergency Response Team. CERT are expert groups that handle computer security incidents. Alternative names for such groups include computer emergency readiness team and computer security incident response team.

DAFUS University of Command & Control of the Islamic Republic of Iran's Army

DCISE Deep Content Inspection System Expansion. Deep Content Inspection (DCI) is a form of network filtering that examines an entire file or MIME object as it passes an inspection point, searching for viruses, spam, data loss, keywords or other content level criteria.

DDoS Distributed denial-of-service. A DDoS attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers.

DoS Denial of service. A DoS attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

FATA Cyber and Information Exchange Police (Iranian Cyber Police).

GSM Global System for Mobile Communications. GSM is a standard developed by the European Telecommunications Standards Institute (ETSI) to describe the protocols for second-generation (2G) digital cellular networks used by mobile phones.

HTTPS Hyper Text Transfer Protocol Secure is the secure version of HTTP, the protocol over which data is sent between a browser and the website being connected to: all communications between the browser and the visited website are encrypted.

ICA Iranian Cyber Army

ICT Ministry of Information and Communications Technology

IP Internet Protocol. IP is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet.

IPDF Iranian Passive Defence Force

IRGC Iranian Revolutionary Guard Corps (Army of the Guardians of the Islamic Revolution).

IRIB Islamic Republic of Iran Broadcasting.

ISP Internet Service Provider: the ISP is a company that provides access to the Internet, usually for a fee.

ITC An organisation affiliated with the Ministry of Information and Communications Technology named 'The Data Company' (currently known as the Information Technology Company, or ITC).

ITRC Iran's Telecommunications Research Centre, currently known as the Information and Communication Technology Research Centre.

MOI Ministry of Intelligence.

MPLS Multiprotocol Label Switching (MPLS) is a mechanism in high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table.

NRI Neda Rayaneh Institute.

OFAC The Office of Foreign Assets Control of the US Department of the Treasury.

P5+1 The P5+1 is a group of six world powers which joined together in diplomatic efforts with Iran with regard to its nuclear programme.

PDO Passive Defence Organisation.

Phishing The attempt to acquire sensitive information such as usernames and passwords by masquerading as a trustworthy entity in an electronic communication.

RAT Remote Access Trojan. A RAT is a piece of software that allows a remote 'operator' to control a system as if they have physical access to that system. Malicious RAT software is typically installed without the victim's knowledge, often as payload of a Trojan horse, and will try to hide its operation from the victim and from security software.

RCDC/Gerdab Revolutionary Guards Cyber Defence Command - Gerdab is the centre for the investigation of organised crime of the IRGC.

SAFAVA Iranian Intelligence and Security Technology Industries

SCC Supreme Council on Cyberspace

SCCR Supreme Council of the Cultural Revolution

Social engineering The psychological manipulation of people in order to trick them into performing actions that would divulge confidential information.

Spear phishing An attempt to acquire sensitive information such as usernames and passwords by masquerading as a trustworthy entity in an electronic communication, tailored and targeted towards a specific individual, organisation or business

TCI Telecommunication Company of Iran

TIC Telecommunication Infrastructure Company

VPN Virtual Private Network – a group of computers (or discrete networks) networked together over a public network – predominately, the Internet. VPNs emerged as the leading circumvention tools used to dodge the Iran's filtering system by Iran's online users.

Introduction

In pursuit of total ideological control, 'The Soft War', the Iranian authorities have gone online in attempts to censor, monitor, and interfere with those who would speak or act against the regime. The exact extent of these efforts remains unknown, as does whether or not the much-discussed 'Iranian Cyber Army' (ICA) does indeed exist. It is clear, however, that there is a set of activities and individuals acting online towards a certain goal: consolidating ideological control, or 'social engineering': using the socio-cultural infrastructure of society to create conformity with the state's ideological mandate.

Since Iran took its first steps into cyberspace in 1993, it has been a regional leader in Internet access and cyber technology. But just months after the Internet was first introduced to the country, the Iranian government began to seek the means to curb the freedom of expression and the free flow of information online. At this moment, the first traces of a regime-led network of online actors emerged: a network supported, if not controlled, by an elite group in Iran's ruling apparatus. Since the widely-disputed 2009 presidential elections, the crackdown on online activity has increased in scope and intensity.

Declarations of the existence of a cyber force have been made by various Iranian authorities and media, and a number of tactics and actors can be positively identified. These tactics range from content-production to invasive hacking, forming a broad picture of the types of activities being undertaken online with the aim of consolidating and increasing state control of discourse, thereby limiting civic space. Regardless of the structure or hierarchy of those individuals and groups responsible, many of these tactics constitute unjustifiable limitations on the right to freedom of expression and the free flow of information, as well as violating privacy and facilitating the persecution and oppression of human rights defenders and activists.

The exact structure and remit of an ICA or online police force is almost impossible to determine: no primary data exists on their organisation or mandate, and their existence has yet to be definitively acknowledged by the Iranian government. Their presence must be traced by following the online footprint that a large body of online actors and computer hackers inevitably leaves behind, and by tracing their relationships and involvement with those official organisations involved in the defence and management of Iranian cyberspace.

The network employs a number of strategies by which it can function covertly: chief amongst these is the use of proxies, which allow the Iranian regime to nominally distance itself from initiatives. The ICA seems to consist of young, tech-savvy IT experts, trained in hacking and surveillance, who are thus permitted to dodge mandatory military service while earning attractive incentives (financial and otherwise). While this network of actors has remained secretive about its structure and direct links to Iranian security and military establishments, it is clear that they enjoy a great amount of support and legal immunity in their work. The activities and priorities appear to directly align with Khamenei's Soft War rhetoric, which they adhere to via mass creation of content and targeting political opposition voices online.

While the Soft War has long formed a part of his rhetoric, in a speech addressing academics on 30 August 2009, Supreme Leader Ayatollah Khamenei spoke of the urgent need to fight an ideological Soft War in the online sphere, a stance perceived as a call to arms by his supporters, and in particular by the Iranian Revolutionary Guard Corps (IRGC), an armed force to protect Iran which also comprises a key element of Iran's Soft War.

A few months before the 2009 Presidential election, the Fars News Agency (an organisation with alleged connections to the IRGC) stated that "ICA belongs to [the] IRGC."[3] The IRGC expanded its political and executive activities early in Ahmadinejad's second term, and began recruiting professionals for its cyber force. In an IRGC Council meeting at Qom province on 20 May 2010, Ebrahim Jabari, the Commander of the Security and Protection Division of the IRGC claimed that they "… have succeeded in setting up a Cyber Army… our Cyber Army is the second strongest in the world."[4]

Soft War rhetoric from Khamenei appears to have triggered a more pro-active approach to Internet censorship, monitoring, and hacking from the authorities, security services, and even grassroots cyber-activists: all employing an approach typified by intimidation and the desire to silence activists, journalists, human rights defenders and those that dissent through constant online attacks. This rhetoric has further legitimised years of efforts to gain control over Iranian cyberspace by government authorities, but also individuals and groups, working alone and in networks, who have long taken it upon themselves to contribute to the strategies set out by Khamenei.

The role of this network of actors cannot be underestimated. With its dedicated taskforce and a broad institutional support, this organisation has harnessed the influence and power of the IRGC to engage in both offensive and defensive censorship of the Internet in Iran. It is clear that the ICA has also been successful in having a chilling effect on freedom of speech online: Iranian authorities have publicised their work with the aim of creating further fear among Internet users in Iran.

[3] CA Belongs to IRGC, Farsnews, May 2009, (online) Available at: http://www.farsnews.com/newstext.php?nn=8802130463 Accessed: 1 March 2016.

[4] RGC Forms Second Cyber Army in the World, Farsnews, May 2010, (online) Available at: http://www.farsnews.com/newstext.php?nn=8902300353 Accessed: 1 March 2016.

The IRGC and ICA

Based on information from sources close to the IRGC, it is clear that the IRGC and the Ministry of Intelligence are, at the very least, involved in the ICA's administration. Following an announcement by government officials on the relationship between the IRGC and ICA, several websites with close ties to the IRGC (i.e. Mashreq) re-published a report by the French newspaper *La Tribune* that the 'IRGC is the authority responsible for policing Iranian cyberspace. In 2009, this powerful arm of the Iranian armed forces took responsibility for controlling the National Internet and has continued doing so ever since. [The] IRGC has established a Cyber Police that oversees the Internet and its users in the country.'[5] In an article published by Fars News in April 2010, Brigadier Ebrahim Jabbari, the head of the Ali ibn Abitaleb Brigade, told a senior official: "Today we witness the successful creation of the ICA by the IRGC forces. Our Cyber Army ranks as second in all the world."[6]

In September 2011, however, the IRGC began to disassociate itself from the ICA, dismissing the ICA as a 'popular and spontaneous grassroots movement'[7] but adding that were it to organise such an entity, it would 'proudly announce the inception of such an army publicly.'[8] To some degree, this announcement contradicted a November 2010 announcement by the IRGC's Vice Director of Cyberspace, who officially declared that "the employees of the Gerdab [Revolutionary Guard Cyber Defence Command / RCDC] website and the collective forces of the IRGC's Organised Crime Division insist that hacking is their last resort and only one part of their online activity. They prefer not to be listed as hackers; nonetheless, hackers can be classified into different levels and groups."[9]

During the peak period of attacks on websites and email accounts of Green Movement activists in March 2010, Fars News Agency published a report about a hacker who called himself a member of the ICA, referring to it as a "division under the supervision of IRGC's non-executive defence forces."[10]

The US State Department currently reports on the presence of several organisations "including the Basij 'Cyber Council', the Cyber Police, and the Cyber Army (presumably operating under the IRGC) that are engaged in surveying and combatting potential cyber threats and 'alleged cyber threats against national security.'"[11] In addition, accounts exist of organised hacking collectives which have been in operation since the early 2000s. There is increasing consensus around the origin and regulation of an ICA, and "a concentrated effort to promote the Iranian government's political narrative online. There have been reports of tenuous links between the ICA and the IRGC, as well as claims that the ICA is a direct offshoot of the IRGC."[12]

There seem to be, however, multiple sources of power and policy for a potential online network of Soft War actors in Iran, including a grassroots element inspired by the rhetoric of Iran's leadership. This makes the policies and activities of such a network even more difficult to track with accuracy.

In September 2013, Hossein Valivand, head of DAFUS (University of Command and Control of the Islamic Republic of Iran's Army), claimed that "…this year, 270 of the crème de la crème of the Army, Navy, Air-force, Khatam-al- Anbiya's Air Defence of the Army, IRGC, Islamic Republic of Iran Police Force and related organisations, such as the office of information and political conscience security of the Army, have registered and enrolled in the cyber security programme. We shall use both hardware and software training, and have for the first time enrolled students in the field of Electronic Warfare in our curriculum."[13] In an interview with the IRIB, Brigadier Hossein Valivand added that "these forces have learned to confront, analyse and prepare a proper reaction against cyber threats."[14]

Furthermore, during a seminar held in early 2013, the general in charge of the Saheb-Al-Amr Army of the Qazvin Division of the IRGC mentioned that "Iran held the 16th place in the world in science last year. Within six years, we will reach 4th place and will also have the 4th strongest Cyber Army in the world."[15] This was supplemented by reports that Iran had officially established a "Cyber War" course in the Military University.

At this point, Khamenei ordered the development of the Iranian Passive Defence Organisation, or PDO, to whom responsibility and management of the ICA should be delegated (according to clauses in the article of association of the PDO). Although the PDO was established in 2003, it was only after Khamenei's directive, in 2014, that it began to be fully developed.[16] The PDO has "played a key role in combating Internet-based threats to the regime since the unrest in 2009."[17] According to Brigadier General Gholamreza Jalali, director of the PDO, the organisation aims to "decrease national vulnerabilities, while increasing stability against foreign threats without the use of arms."[18]

Other units and organisations involved in Iran's cyberspace include the Cyber and Information Exchange Police (FATA), established in April 2011 to monitor and prosecute potential cyber criminals;[19] and the Cyber Defence Command, an organisation run by the Iranian Revolutionary Guard Corps (IRGC), which maintains control over access to online content by Iranian Internet users. Additionally, in July 2012, the Representative of the Basij Chief Commander reported that a "cyber army" would be founded by the Basij, and that Basiji hackers would "attack websites run by the enemies of the Islamic Republic". The Commander of the Islamic Republic of Iran Broadcasting (IRIB) Basij announced that a "base" and two "cyber battalions" would be established to "fight our enemies in cyber war".[20]

[5] What Does a 250,000 Member ICA Have in Mind, Mashreghnews, September 2011, (online) Available at: http://www.mashreghnews.ir/fa/print/64789 Accessed: 1 March 2016.

[6] IRGC Has Developed World Second Largest Cyber Army, Farsnews, May 2010, (online) Available at: http://www.farsnews.com/newstext.php?nn=8902300353 Accessed: 1 March 2016.

[7] NO ICA in IRGC Organisational Chart, Nasim Online, September 2011, (online) Available at: http://old.nasimonline.ir/NSite/FullStory/News/?Id=268650 Accessed: 1 March 2016.

[8] ICA is Organised by Basij, Not IRGC, ITNA, September 2011, (online) Available at: http://itna.ir/vdcexe8z.jh8ovi9bbj.html Accessed: 1 March 2016.

[9] War Declaration to White Hackers, Gerdab, November 2010, (online) Available at: http://www.gerdab.ir/fa/print/2723 Accessed: 1 March 2016.

[10] ICA from A to Z, Farsnews, February 2010, (online) Available at: http://www.farsnews.com/printable.php?nn=8812040390 Accessed: 1 March 2016.

[11] Country Information and Guidance, Iran: Journalists and Bloggers, Home Office, October 2014, (online) Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/362260/CIG_-_Iran_-_Journalists_and_Bloggers_-9_October_2014.pdf. Section 2.1.3 Accessed: 1 March 2016.

[12] After the Green Movement: Internet Controls in Iran, 2009-2012, OpenNet Initiative, 2013. P. 94.

[13] DAFUS is the Most Secure State University, IRNA, August 2013, (online) Available at: http://www.irna.ir/fa/News/81714517/ and http://goo.gl/f9EOjv Accessed: 1 March 2016.

[14] Cybersecurity Curricula Developed for DAFUS, IRIB News, (online) Available at: http://www.iribnews.ir/NewsText.aspx?ID=437556 and http://goo.gl/f9EOjv Accessed: 1 March 2016.

[15] ICA Will Achieve the 4th Place in the World, Mashreghnews, January 2013, (online) Available at: http://www.mashreghnews.ir/fa/print/187118 Accessed: 1 March 2016.

[16] Supreme Leader Approves PDO Article of Association, Mehrnews, Januarry 2015, (online) Available at: http://goo.gl/E2I1a3 Accessed: 1 March 2016.

[17] ICT Ministry Refuses to Block Whatsapp, Gerdab, September 28, 2014, Accessed: 1 March 2016. http://goo.gl/VqBIPV - ICT Minister then added that he acted based on a direct order of President Rouhani. Please see: http://goo.gl/8QFkjb.

[18] Ibid.

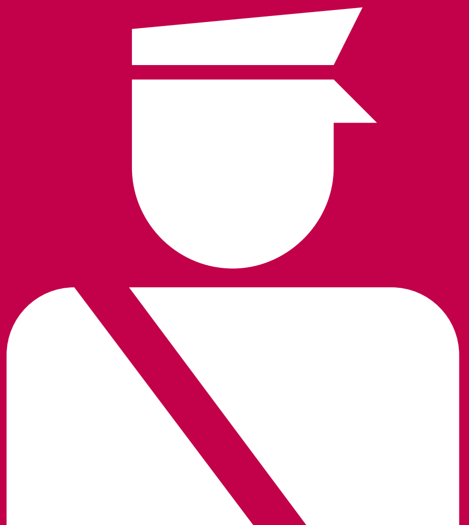
[19] ARTICLE 19 previous reports on Computer Crimes Law (2012), Online Risky Behavior (2015), National Internet (Forthcoming).

[20] One Base and Two Armies for Soft War, Roozonline, July 2011, (online) Available at:http://www.roozonline.com/persian/news/newsitem/article/-6ece7eab90.html, Accessed: 1 March 2016.

"Iranian Anonymous" released a series of documents titled 'Operational deployment plan of the Information Security Management of the IRGC' which provides a detailed analysis of Iran's move towards 'Cyber Warfare'. The group claims that the cost of a cyber weapon can typically range between $300 and $50,000 USD, highly cost effective when compared to the costs of military hardware. Thus, increasing attention to cyber campaigns is both economically justifiable and an efficient use of resources. Such an investment can pay dividends in other domains of warfare, providing a force-multiplier effect when applied in conjunction with space, air, sea, and ground missions.

Iranian Anonymous also published a document outlining the recommendations of the Iranian Intelligence and Security Technology Industries (SAFAVA) relating to strategic cyber defence and cyber warfare strategies: SAFAVA claim that Iran is facing a full-scale intelligence war.

Section 1
Iran and the Internet – a brief history



Early tactics were focused on technical filtering and monitoring of the Internet by state bodies, and the development of a domestic infrastructure which would facilitate further Internet control in the long term. Subsequently, tactics have included creating new legal norms and legal institutions with the aim of promoting a national and government ideology, as well as surveillance and invasive measures. The roots of an online strategy for social engineering, or ideological control, can be traced back to the very beginning of Internet access in Iran.

Early History

Iran continues to grow as an online force, and has long been one of the regional leaders in Internet access and cyber technology: its online presence dates back to the Internet's early days. In 1993, Massoud Saffari, Head of the High Council of Informatics, suggested creating a dedicated data communications network, using the country's existing telephone infrastructure.[21] Iran's first commercial Internet Service Provider (ISP) was established soon after, and the non-profit Neda Rayaneh Institute (NRI), an affiliate of the municipal government of Tehran, began offering Internet access in February 1995.[22]

See Appendix 1

Just six months later, the Iranian government was seeking methods of curbing access to information presented by this new medium. In early August 1995, all 200 of NRI's dial-up lines were disconnected by the Telecommunications Company of Iran (TCI).[23] Though connections were soon restored, it was an unmistakable signal of the government's willingness to control online activities: online expression would be martialled and monitored just the same as offline expression was.

The Iranian telecommunications sector has been structured and developed to facilitate such government intervention: the Ministry of Information and Communications Technology (ICT) directly controls the Telecommunication Infrastructure Company (TIC), which has a "monopoly over the purchase of international Internet gateways in Iran."[24]

2009 Elections

The widely-disputed 2009 elections and their immediate aftermath, including the rise of online communication and content as part of the 'Green Movement', were met with a crackdown on expression online: a response to the surge in usage of online fora and communications for expressing dissent and civic organisation.

While campaigning for the 2009 presidential elections, Mehdi Karoubi and Mir-Hossein Mousavi, the rivals of regime-backed candidate Mahmoud Ahmadinejad, both had strong online presences. Throughout the election period, however, almost all of the websites related to or supporting Mousavi were blocked, leading to public outrage.[25]

During this period, the government also attempted to filter messenger applications such as Google Chat, Yahoo Messenger and Messenger.[26] In several instances, Internet connections were completely severed, preventing communication and any reporting of events. Mobile phone services were also shut down during periods of the 2009 demonstrations.[27]

During his tenure as President, Ahmadinejad repeatedly filtered websites and decreased Internet speeds, a practice which encouraged the formation of a social protest movement, the Green Movement, after the 2009 elections, whose magnitude posed a considerable challenge to the regime. Throughout his term, Ahmadinejad's government not only filtered numerous websites and threatened legal action against website managers and owners, but also deliberately decreased Internet speed to such an extent that many websites became inaccessible. For home use, Internet speeds were reduced to 128kbps, effectively cutting off access.[28]

In particular since the emergence of the Green Movement, the authorities have cracked down on online activity. This has included blocking popular websites, and in some cases creating Farsi-language alternatives such as a government-led "National Email" service. The government's online response to the emergence of the Green Movement was broad: they even blocked the name of the month in which the protests had taken place ("Bahman") from showing up in search engine results.[29]

President Rouhani

When Hassan Rouhani took over the Presidency in 2013, the public hoped that censorship of online content would stop. However, despite his assurances that Iranian citizens have the right to digital freedom, Rouhani is currently developing a new filtering strategy known as 'smart filtering', and his otherwise softer approach to the Internet has been undermined, having been met with resistance from state bodies including the judiciary itself.[30]

The cessation of Internet censorship was one of the public demands during Hassan Rouhani's Presidential campaign. When Rouhani came to power in 2013, however, there was a legal indictment issued against Facebook and Twitter as conspirators in the 2009 protest movement, stipulating that use of such websites is a crime: a legacy of the previous regime.[31] Iranian Internet Service Providers (ISPs) were instructed to block these websites, and a new filtering strategy was put in place.[32]

Rouhani himself seemed to take a softer approach towards Facebook and Twitter. Rouhani and several of his cabinet ministers, including the Minister of Foreign Affairs, Javad Zarif,[33] First Vice-President Eshagh Jahangiri, and Minister of Islamic Culture and Guidance, Ali Janati, started using

[21] Burkhart, Grey E., National security and the Internet in the Persian Gulf Region, June 28, 1998.

[22] Ibid.

[23] Ibid.

[24] After the Green Movement: Internet Controls in Iran, 2009-2012, OpenNet Initiative, 2013.

[25] New Round of Filtering in Iran, Hamvatan Salam, April 4, 2009, (online) Available at: http://www.hamvatansalam.com/news128805.html; and, Facebook Is Finally Filtered, ITNA, May 24, 2009, (online) Available at: http://www.itna.ir/vdcc0eqs.2bqix8laa2.htm, Both accessed: 1 March 2016

[26] Known disruptions of traffic to Google products and services, Google Transparency Report, (online) Available at: https://www.google.com/transparencyreport/traffic/disruptions/#region=IR&expand=Y2012,Y2011,Y2010,Y200g Accessed: 1 March 2016.

[27] Jaras website on three occasions: http://www.rahesabz.net/story/6563/; http://www.rahesabz.net/story/6517/; http://www.rahesabz.net/story/6872/ Accessed: 1 March 2016.

[28] Iran Cuts Internet Speeds to Homes and Cafes, NBC News, October 18, 2006, (online) Available at:http://www.nbcnews.com/id/15318455/ns/world_news-mideast_n_africa/t/iran-cuts-Internet-speeds-homes-cafes/
Accessed: 1 March 2016.

[28] Iran opposition planning protests, Aljazeera, February 13, 2011, (online) Available at: http://www.aljazeera.com/news/middleeast/2011/02/201121216252615O718.html Accessed: 1 March 2016.

[29] The Judiciary Decision on Facebook, Fararu, December 2013, (online) Available at: http://fararu.com/fa/news/170943 Accessed: 1 March 2016.

[30] Bill of Indictment for Second Accused Group of Color Coup, Farsnews, August 2009, (online) Available at http://www.farsnews.com/newstext.php?nn=8805170594 Accessed: 1 March 2016.

[31] ARTICLE 19, Legal Analysis: Computer Crimes Law, 2012, (online) Available at: https://www.article19.org/data/files/medialibrary/2921/12-01-30-FINAL-iran-WEB%5B4%5D.pdf Accessed: 1 March 2016.

[32] Rezaian, Jason, Iran's Rosh Hashanah tweets could herald new openness, *the Guardian*, September 2013, (online) Available at: http://gu.com/p/3ttqb/stw Accessed: 1 March 2016.

[33] Kamali Dehghan, Saeed, Hassan Rouhani suggests online freedom for Iran in Jack Dorsey tweet, *the Guardian*, October 2013, (online) Available at: http://gu.com/p/3j8t6/stw Accessed: 1 March 2016.

Facebook and Twitter to communicate with Iranian citizens and the wider world. In a notable public twitter exchange, Rouhani told Twitter co-founder Jack Dorsey that he believed in Iranians' right to digital freedom.[34] In a meeting with members of Tehran's Chamber of Commerce, Ali Janati promised that the filtering of Facebook and other social media sites would be lifted. He called the censorship "ridiculous", stating: "if we look back at the actions we took we find some ridiculous decisions. For instance, the bans on VCR, VCR tapes or even fax machines!"[35]

[34] Kamali Dehghan, Saeed, Hassan Rouhani suggests online freedom for Iran in Jack Dorsey tweet, *the Guardian*, October 2013, (online) Available at: http://gu.com/p/3j8t6/stw Accessed: 1 March 2016.

[35] The Prohibitions are "Ridiculous", Roozonline, March 2014, (online) Available at: http://www.roozonline.com/persian/news/newsitem/article/-6a00ec05e3.html Accessed: 1 March 2016

Section 2 Information Online – filtering, smart filtering and monitoring

Introduction

Given Iran's religious dictates, there has always been concern over domestic and international information flows, in particular when addressing matters of 'illicit content', 'cultural imperialism', and 'subversive' speech.[36] Foreign Minister Javad Zarif, who stated, "there is stuff on the Internet that people have access to that is as offensive as The Satanic Verses and it is updated every day. We believe a certain level of decency must be provided."[37]

As well as interfering with access to information on a technical level, with service shutdowns (see Section 1), the regime has interfered with the free flow of information in Iran, both preventing the sharing and discussion of ideas, and the online organisation and coordination of social action such as protest or meetings, further interfering with the right to freedom of association.

The government has combated perceived ideological challenges (i.e. waged their Soft War) with a combination of defensive and offensive content strategies, combining a complex network of censorship with a specific body of promoted pro-government content the aim of which is to provide a pro-government national alternative to content that is viewed as dissenting or treasonable, while simultaneously suppressing that content.

The intensity and scope of such activities has increased markedly since the 2009 Green Movement, which saw the widespread use of social networks as a tool for mobilisation and collective action. To counter this trend, the government has implemented monitoring and filtering techniques, alongside a far-reaching legal framework, to aid the prosecution of those suspected of undesirable online expression and activities.

Bandwidth throttling

Iran is one of few governments which deliberately limits Internet speed ('bandwidth throttling') for the purpose of controlling citizens' access to online content. Iran's Internet speed is among the slowest in the world:[38] for home use, Internet speeds have been reduced to 128kbps, effectively cutting off access.[39]

Blocking & filtering

The difference between 'blocking' and 'filtering' is a matter of scale and perspective. 'Blocking' often refers to preventing access to resources in the aggregate, while 'filtering' refers to preventing access to specific resources within an aggregate.[40]

Iran has blocked and filtered almost a quarter of all websites worldwide.[41] Filtering has become a common practice of the Iranian authorities, especially during times of protest: in 2012, following a repeat of the previous year's demonstrations, all Gmail, Yahoo Mail and HTTPS sites were blocked from the early hours of 9 February.[42] In reaction to this, the head of the Islamic Parliamentary Research Centre, Ahmad Tavakoli, warned of the consequences of "Abusive Filtering", calling the action a "waste of resources", and asking for an explanation.[43] Even Raja News, one of the websites that supported the government, protested against the filtering and was filtered itself.[44]

Iran's 2000 Publication Law was amended to stipulate that all news websites and electronic publications must receive permits to operate. Failure to observe this amendment (i.e. publish online without a permit) would result in the website being filtered, and would be considered a criminal offence. As a result of this law, the following websites were either temporarily or permanently filtered: Google,[45] Bing,[46] Facebook, Twitter,[47] former President Rafshanjanisi web page,[48] former President Khatami's web page,[49] Saham news,[50] Persian blog,[51] Blogfa,[52] Blogger,[53] Wordpress,[54]

[36] Burkhart, Grey E., National security and the Internet in the Persian Gulf Region, 28 June, 199

[37] Ibid.

[38] Ibid.

[39] Iran Cuts Internet Speeds to Homes and Cafes, NBC News, 18 October, 2006, (online) Available at: http://www.nbcnews.com/id/15318455/ns/world_news-mideast_n_africa/t/iran-cuts-Internet-speeds-homes-cafes/ Accessed: 1 March 2016.

[40] See https://tools.ietf.org/html/rfc7754.

[41] Seifi, Farnaz, Internet in Ahmadinejad Term, *Deutsche Welle,* Oct. 2013, (online) Available at: http://dw.com/p/19NCH ; Accessed: 1 March 2016. Article 19 cannot verify the figures provided in the DW report.

[42] See: http://yro.slashdot.org/story/11/10/06/1328211/iran-blocks-vpn-ports and https://news.ycombinator.com/item?id=3575029; Gmail and Ymail Shut Down, Entekhab, February 20, 2012, (online) Available at: http://goo.gl/vp61o0, Accessed: 1 March 2016 Email Services Shut Down and Reopened, Alef, February 20, 2012, (online) Available at: http://alef.ir/vdcbwab80rhba8p.uiur.html?144186 and Who wants the Internet Blocked?, TABNAK, February 20, 2012, (online) Available at:, http://goo.gl/PwcqQl, Known disruptions of traffic to Google products and services, Google Transparency Report, (online) Available at: https://www.google.com/transparencyreport/traffic/disruptions/#region=IR&expand=Y2012,Y2011,Y2010,Y2009. All websites accessed: 1 March 2016

[43] Illegal Filtering Brings Costs, TABNAK, February 12, 2012, (online) Available at: http://goo.gl/tqwFrf Accessed: 1 March 2016.

[44] Pro-Government Blogs Filtered, BBC, April 29, 2010, (online) Available at http://www.bbc.com/persian/iran/2010/04/100429_l07_iran_rajanews_filtering_cyberspace.shtml Accessed: 1 March 2016.

[45] Google Filtered, Khabaronline, May 28, 2010, (online) Available at: http://www.khabaronline.ir/detail/64863 Accessed: 1 March 2016.

[46] Ibid.

[47] Facebook and Twitter Filtered, Khabaronline, May 23, 2009, (online) Available at: http://www.khabaronline.ir/detail/8977/ Accessed: 1 March 2016.

[48] Why Rafsanjani's Website was Filtered, Mehrnews, January 2, 2012, (online) Available at: http://goo.gl/H4fS3q Accessed: 1 March 2016.

[49] Khatami Banned from Political Activity, BBC, November 5, 2010, (online) Available at: http://www.bbc.co.uk/persian/iran/2010/11/101104_u03_khatami_website_filtered.shtml Accessed: 1 March 2016.

[50] Sahamnews Filtered, Farsnews, August 30, 2009, (online) Available at: http://www.farsnews.com/newstext.php?nn=8806080245, Accessed: 1 March 2016.

[51] Persianblog Filtered, Farsnews, June 20, 2010, (online) Available at: http://www.farsnews.com/newstext.php?nn=8903301033, Accessed: 1 March 2016.

[52] Blogfa Filtered, Farsnews, June 20, 2010, (online) Available at: http://www.farsnews.com/newstext.php?nn=8903300921, Accessed: 1 March 2016.

[53] Blogger Filtered, ITNA, April 26, 2010, (online) Available at: http://itna.ir/vdcbawb8.rhbf0piuur.html Accessed: 1 March 2016.

[54] Wordpress Filtered, Asriran, February 10, 2011, (online) Available at: http://www.asriran.com/fa/print/155914 Accessed: 1 March 2016

Khabar online,[55] Travin,[56] WeChat,[57] and the website of the British Embassy in Tehran, Iran.[58]

Other websites to be filtered included Persian Wikipedia, which was filtered at midnight on 3 October 2010, though the filter was withdrawn the following day.[59] Gmail and many Google services were filtered on 23 September 2012 following the publication of an Anti-Islamic video on YouTube and YouTube's refusal to remove it.[60] Of the 946 total filtered pages, 414 were filtered due to social and political content, 189 for sexuality, 137 for religious content, and 97 regarding human rights issues.[61]

Ahmadinejad's 9th and 10th Administrations created Farsi-language alternatives to some blocked websites, creating "Aparat"[62] as a localised YouTube, and offering "Face-Nama"[63] as a local version of Facebook. The government also initiated a "National Email" service. However, after several years of investment in localised services, most of the alternatives were abandoned due to a lack of traffic, and a failure to draw users away from the original product.

'Smart Filtering'

After winning the presidential elections, Rouhani's government undertook a new filtering strategy. Mahmoud Vaezi, Rouhani's Information and Communications Technology Minister, stated that the government did not intend to filter all websites. He referred to their plan as 'smart filtering' and explained: "smart filtering means to put immoral and criminal content out of reach"; There is also some suggestion 'smart filtering' relates to security criteria as well as content: "Along with the growth and development in localisation of cyberspace, we also turned to smart filtering to provide our people with a higher level of security."[64]

Speaking on the status of the smart filtering project, Vaezi added that they were collaborating with a 'reputable' university in the country. Some reports indicate mobile operators will be subject to smart filtering, and that agreements worth $37 million have been reached with 11 universities to invest in required research and technology.[65]

[55] Khabaronline Filtered, Alef, December 21, 2011, (online) Available at: http://alef.ir/prtb9sb8arhbf5p.uiur.html Accessed: 1 March 2016.

[56] Online Game Travian Filtered, Farsnews, January 2, 2013, (online) Available at: http://www.farsnews.com/newstext.php?nn=13911013000562 Accessed: 1 March 2016.

[57] WeChat might Become Unfiltered, CITNA, December 23, 2013, (online) Available at:http://www.citna.ir/news/11683 Accessed: 1 March 2016.

[58] UK Embassy Website Filtered, Mehrnews, December 22, 2011, (online) Available at: http://www.mehrnews.com/print/1490656/ Accessed: 1 March 2016.

[59] Wikipedia Farsi Filtered and Unfiltered, TABNAK, October 3, 2010, (online) Available at: http://www.tabnak.ir/fa/pages/?cid=123241, Accessed: 1 March 2016.

[60] Google and Gmail Filtered, TABNAK, September 23, 2012, (online) Available at: http://www.tabnak.ir/fa/print/274345 and http://gu.com/p/3aj6p/stw Accessed: 1 March 2016.

[61] Shaheed, Ahmed, Censoring the Commons: Internet Freedom curtailed on Wikipedia, November 2013, (online) Available at: http://shaheedoniran.org/english/english/censoring-the-commons-internet-freedom-curtailed-on-wikipedia/ Accessed: 1 March 2016

[62] See http://www.aparat.com/etc/blog/one/postid/20

[63] See http://facenama.com/home

[64] Government Seeks Smart Filtering, Farsnews, February 2015, (online) Available at: http://www.farsnews.com/newstext.php?nn=13931113001048 Accessed: 1 March 2016.

[65] Mobile Operators Subject to Smart Filtering, Tabnak, February 2016, (online) Available at: http://goo.gl/AQiVPr Accessed: 1 March 2016

On 19 December 2013, the application WeChat and its website were filtered by the CCDOC (Committee Charged with Determining Offensive Content).[66] The CCDOC elaborated on the reasons behind the censorship: "the application was a security and privacy breach for mobile phone users and stole important information from users' phones. In addition, this application was the source for the distribution of immoral content and pornographic materials that are harmful to the youth. Since the manufacturers of this application are outside of the country and have no regards to the complaints from the families of these young people, CCDOC has unfortunately decided to filter the application. We are confident that young people can find a similar, locally available application for audio, text, video and visual communication."

Vaezi stated that his Ministry had nothing to do with the filtering of WeChat, adding that the CCDOC has a 12-member board, at which Vaezi holds only one place. He stated that his Ministry has recommended that the censorship on WeChat be lifted: "Right now many people are using this application in a correct way. The difference of WeChat to other social network application/sites is that it has an option called 'nearby' that may be used incorrectly. We have recommended that this part of the application to be filtered and the other options be available for public use."[67]

Agencies involved in filtering

Websites are, theoretically, blocked based on decisions made by CCDOC, under the judiciary's supervision. Khamenei has a significant role in appointing senior officials within these agencies, and in 2012 was responsible for establishing the Supreme Council of Cyberspace (SCC), which is the highest-ranked authority in the field of online access to information, and is responsible for developing general guidelines for cyberspace governance.

The CCDOC constantly updates a list of websites that need to be filtered: this is done by constantly searching for new websites and content as they become available. They are assisted in this regard by Iran's Telecommunication Company, which itself outsources some of the monitoring to ISPs[68] who all have to buy bandwidth from this company.[69] ISPs are all monitored by the Communications Regulatory Authority,[70] which legally requires the implementation of guidelines developed by the CCDOC.[71]

The CCDOC functions as a bridge between policy and implementation: its role is to determine illegal content on the web, and provide authorities (including the ICT Ministry, Telecommunication Company of Iran,[72] Telecommunication Infrastructure Company) with a list of websites that must be blocked, based on certain criteria. These criteria include subverting social norms, breaking Islamic rules, threats to national security, and promotion of techniques that can be used to circumvent censorship.[73] It is closely connected to, and shares members with, the SCC, but functions under the supervision of the Office of the Prosecutor General.

[66] See: http://web.archive.org/web/20131224121333/http://Internet.ir/faq.html Accessed: 1 March 2016.

[67] Communication Minister Wants WeChat Unfiltered, Fararu, December 2013, (online) Available at: http://fararu.com/fa/print/173969, Accessed: 1 March 2016.

[68] Internet Censorship in Iran, Iran Media Program, March 18, 2013, Accessed: 1 March 2016. http://iranmediaresearch.org/en/research/pdffile/1296 Accessed: 1 March 2016.

[69] New list of Filterings reduces speed of Internet, Donyayeh Eghtesad, http://donya-e-eqtesad.com/news/387150 Accessed: 1 March 2016.

[70] See: www.cra.ir.

[71] Aryan, Simurgh, and Aryan, Homa, and Halderman, Alex, Internet Censorship in Iran: A First Look, August 2013, Available at: https://jhalderm.com/pub/papers/iran-foci13.pdf Accessed: 1 March 2016.

[72] See: https://www.tci.ir/ Accessed: 1 March 2016.

[73] See: http://www.tic.ir/#home Accessed: 1 March 2016.

The CCDOC is composed of representatives from the Ministry of Education, the Ministry of Information and Communications Technology, the Ministry of Intelligence, the Ministry of Justice, the Ministry of Science, Research, and Technology, the Ministry of Culture and Islamic Guidance, the Islamic Development Organisation, as well as the president of the Islamic Republic of Iran Broadcasting (IRIB), the Chief Police Commander, an expert on communications and information technology appointed by the Industry and Mine Commissions in the Islamic Consultative Assembly (Majlis), and a representative of the Assembly appointed by the Legal and Judicial Commission and approved by the Assembly. The CCDOC meetings are presided over by the Prosecutor General.[74]

Blocking and filtering has, however, been authorised and implemented outside of this official process: indeed it would seem that in practice multiple powercentres have the authority to block and filter online content. There have been instances in which websites were blocked or offices shut down by a direct order from the judiciary without any intervention from the CCDOC.[75] Additionally, the Ministry of Culture and Islamic Guidance has directly been involved in filtering, with the permission from the Supreme Council of National Security, with no CCDOC involvement.[76] There have also been instances where the Minister of Information and Communications Technology has refused to implement filtering orders received from the CCDOC.[77]

Filtering evidence of hacking?

In May 2016, Palo Alto Networks published the report “Prince of Persia”, a report identifying the activities of a hacking group named ‘Infy’; subsequent actions taken by telecommunications regulators made the report unavailable online inside Iran, with activities indicating either an intervention to end operation of the Infy network or an attempt to interfere with further research. This filtering is conducted at the primary international gateway maintained by the Telecommunication Company of Iran: as Claudio Guarnieri and Collin Anderson note, that though the reasons for the filtering are not immediately clear, “the filtering policy indicates that Iranian authorities had specifically intervened to block access to the command and control domains of a statealigned intrusion campaign at a country level.”[78]

[74] Meet the Filtering Committee Members, Khabaronline, October 27, 2015, Available at: 1 March 2016. http://www.khabaronline.ir/detail/472007/ict/Internet Accessed: 1 March 2016.

[75] “The Third Wave” Website and Office Shut Down, Mowjnews, June 13, 2009, Available at: https://goo.gl/8TMxqo Accessed: 1 March 2016.

[76] CCDOC Complaint Appealed, IT Iran, May 17, 2015, Available at: http://itiran.com/d/68668 Accessed: 1 March 2016.

[77] ICT Ministry Refuses to Block Whatsapp, Gerdab, September 28, 2014, Available at: http://goo.gl/VqBIPV Accessed: 1 March 2016.- ICT Minister then added that he acted based on a direct order of President Rouhani. Please see: http://goo.gl/8QFkjb Accessed: 1 March 2016.

[78] Claudio Guarnieri & Collin Anderson, Iran and the Soft War for Internet Dominance, Black Hat USA, August 2016 pp 19-20 – available at: https://iranthreats.github.io/us-16-Guarnieri-Anderson-Iran-And-The-Soft-War-For-Internet-Dominance-paper.pdf Accessed: 1 March 2016.

Section 3 Monitoring, prosecutions, and shrinking civic space

Introduction

As early as 2001, the Supreme Council of the Cultural Revolution (SCRC) began to implement a series of regulations that required ISPs to employ filtering systems, monitor and record customers' internet use, and remove all anti-government and anti-Islamic websites from their servers.[79]

Iran enforces numerous laws specifically restricting expression of speech, including the Press Law 1986, the Computer Crimes Law 2010 is one of the principle tools for prosecution for activities online: the provisions are broad, disproportionate, and in clear contradiction of international standards. For more on Iran's legislative framework to restrict online expression, see ARTICLE 19's legal analysis and reports.[80]

Though there are significant levels of phishing (see below) targeted at civil society, it is worth noting that much of the information gained online which enables prosecutions of communicators and activists is gained in a legal manner, i.e. from data publicly available on social media: many activists fail to take adequate security measures to protect their anonymity and data online. *"During my interrogation, I realised that whatever information the authorities claimed to have on me had been gathered from my Facebook page, or [the pages] of my friends where I am tagged,"* stated an Iranian activist interviewed by ARTICLE 19 for the 'Risky Online Behaviour' Report. [81]

Case study

Naghmeh Shahsavandi spent 75 days in Evin prison (Section 2A) in 2013, released on $600,000 USD bail. She was subsequently sentenced to seven years in jail for insulting the Supreme Leader, insulting the founder of the Islamic Republic, and colluding against the regime. She was sentenced to an additional 91 days for publishing pornographic material online, and was accused of being the administrator of a Facebook page which had more than four million likes.[82]

The most important question is how activists are exposed and identified: the most common answer is carelessness online. Shahsavandi stated that she was not familiar with online security or the possibility of attack by hackers. In order to bypass online censorship, she used VPN accounts which were publicly available on the local black market, and paid for them using the local banking system.[83] When she heard about other activists being arrested, she handed the management of her accounts to an individual outside the country. Upon her arrest she realised that she had been under surveillance, and that all of her text messages had been intercepted by the authorities.[84]

Shahsavandi described her ordeal: "Most of the interrogations were concerned with details about my private life. They put a lot of pressure on me to obtain the names of the other system administrators and pressured me to incriminate my associates. They even brought us together to confront each other. They would film the interrogations and asked me questions about the details."[85]

[79] See http://www.Iranhrdc.org/English/English/publications/reports/3157-ctrl-alt-delete-iran-039-s-response-to-the-internet.html?p=1 Accessed: 1 March 2016 and ARTICLE 19's Risky Online Behaviour Report for more.

[80] Iran's Computer Crimes Law, Legal Analysis, available at: https://www.article19.org/data/files/medialibrary/2921/12-01-30-FINAL-iran-WEB%5B4%5D.pdf; Risky Online Behaviour, available here https://www.article19.org/data/files/medialibrary/38039/Risky-Online-Behaviour--final-English.pdf Accessed: 1 March 2016.

[81] ARTICLE 19, Risky Online Behaviour, ibid, p23.

[82] Shahsavandi: I was told I have 4 million 'likes' and that disturbs National Security, International Campaign for Human Rights in Iran, August 2015, (Online) Available at: http://persian.iranhumanrights.org/1394/05/shahsavandi-facebook-sentenced/ Accessed: March 1, 2016, 83 Ibid.

[83] Ibid.

[84] Ibid.

[85] International Campaign for Human Rights in Iran, Ibid.

However, the judiciary itself engages in the monitoring of cyberspace and users' activities in chats and online environments.[86] As an authority responsible for monitoring Iranian cyberspace, the judiciary plays the most significant role in enforcing filtering policies and responding to violations of relevant laws in Iran; however, a month after a press interview by the judiciary's Deputy in Cultural Affairs, 2,600 judges were prepared to start engagement in chats and cyberspace.[87] According to Hadi Sadeghi, the judiciary's Deputy in Cultural Affairs, one factor that motivated this organisation to get involved in cyberspace was "the requirement to bridge the legal gap and cover loopholes in the cyberspace."

Sadeghi drew a parallel with traditional physical warfare, referring to a lack of knowledge regarding 'cyberspace' and adding that the judiciary should refocus its attention on this environment. "This situation resembles the one we encountered during the Iran-Iraq war, in which we were empty-handed in fighting Saddam and the Ba'th regime, who were armed to the teeth; while in that tough war we could stop the enemy by sacrificing ourselves physically, today we should replace those old techniques with new ones to achieve success in the cyber war."

"In this situation, we should know, before anything, what is happening in cyberspace so that we can use our knowledge, science, and persistence to defeat our enemy in the soft war."[88]

Following a wave of censorship and the closure of several prominent print publications in the early 2000s, blogs became a key means for people to express their thoughts and viewpoints.[89] The additional closure of newspapers and news websites created a vacuum, in which people turned to blogs to express their ideologies and share their beliefs. 'Blogging fever' began in 2001 following the publication of the first Farsi blog by Salman Hariri, with a huge variety of individuals and interests forming the blogosphere[90]

Blogs have been filtered and bloggers incarcerated during the presidencies of Khatami, Ahmadinejad, and Rouhani. Several notable bloggers, such as Mehdi Khazali,[91] Sina Motalebi,[92] Mojtaba Saminejad,[93] Hossein Derakhshan,[94] and Sattar Beheshti (who died in custody in November 2012), have all been prosecuted as an indirect result of their online activities.[95] In 2010 alone, Iran arrested 50 bloggers, placing Iran in the bottom ten countries in Freedom House's index for online freedom of expression.[96]

[86] Launch of the Judiciary's Social Network, Pajvak, September 2015, (online) Available at: http://goo.gl/pUoR58 Accessed: 1 March 2016.

[87] The Judiciary Enters Chat Space, Mehrnews, October 2015, (online) Available at: http://goo.gl/HwnefE Accessed: 1 March 2016.

[88] Filling the Legal Gap in Cyberspace, ISNA, September 2015, (online) Available at: http://goo.gl/uitcMa Accessed: 1 March 2016.

[89] Examples are closure of Jamepl, Salam, Aftab Emrooz, Sobh e Emrooz, Asr e Azadegan Newspapers amongst others. For details please visit: http://www.bbc.com/persian/arts/story/2008/02/080205_mf_jameah.shtml and http://www.bbc.com/persian/iran/story/2004/07/040706_a_mb_salam_newspaper.shtml and http://www.peiknet.net/03-05/s_Vaazin_s_m_nah_g_m.htm.

[90] Interview with First Iranian Blogger Salman Jariri, BBC, April 28, 2010, (online) Available at: http://www.bbc.com/persian/iran/2010/04/100428_l50_salman_jariri_vid.shtml Accessed: 1 March 2016.

[91] 14 Years Imprisonment and 10 Years Exile for Mehdi Khazali, BBC, February 5, 2012, (online) Available at: http://www.bbc.com/persian/rolling_news/2012/02/120205_rln_l21_khazali_prison.shtml Accessed: 1 March 2016.

[92] Three journalists transferred to notorious "special wing" of Evin prison; exiled journalist's father arrested, ifex, September 14, 2004, (online) Available at: http://www.ifex.org/en/content/view/full/61261, Accessed: 1 March 2016.

[93] See: https://en.wikipedia.org/wiki/Mojtaba_Saminejad.

[94] Iran blogger Hossein Derakhshan temporarily released, BBC, December 9, 2010, (online) Available at: http://www.bbc.com/news/world-middle-east-11962032 Accessed: 1 March 2016.

[95] Kamali Dehghan, Saeed, Iran accused of torturing blogger to death, The Guardian, November 8, 2012, (online) Available at: www.theguardian.com/world/2012/nov/08/iran-accused-torturing-blogger-death Accessed: 1 March 2016.

[96] Freedom of the Press: Iran, Freedom House, 2010, (online) Available at: https://freedomhouse.org/report/freedom-press/2010/iran Accessed: 1 March 2016.

Alireza Shirazi, the Managing Director of Blogfa and Parsak blog sites, wrote on his personal blog in 2009: "In recent months and especially in the last few weeks, due to the increasingly complicated political situation in the country and the ratification of the Computer Crimes Law, many weblogs have been closed down or blocked. I am not in a position to judge the content of these weblogs, but the sheer number of weblogs closed by the authorities shows that the rate of censorship has increased by the factors of ten in comparison to the last few years."[97]

Alireza Shirazi (Blogfa and Parsik), Mohammad Javad Shakoori (Mihan Blog and Cloob), and Masoud Changizi (Blog Sky and Pikofile), managers of some of the most popular blogs in Iran, issued a joint statement in Autumn 2010 in which they drew attention to the government's increasingly evident role in blocking websites and blogs. They also stated that "the role of [the CCDOC] is … to redefine online crime and try to purify the cyberspace. Website and blog providers are also required to obey the laws and take action when necessary. Any other procedure is not the responsibility of the CCDOC. Recently, however, it appears that the CCDOC not only defines the crime but also takes action and interferes with the management of service providers. Threats, intimidation, and judicial prosecution accompany some of these acts of interference."[98]

In its role as "protector of national security in the cultural and social arena," the IRGC is responsible for overseeing and controlling cyberspace, finding the culprits (organised criminals or otherwise) accused of subverting cultural and social standards, and initiating a warrant for their arrest when necessary.[99] An initial project was called 'Mozelin' ('the Perverts' in English), and led to the closure of several websites and weblogs in 2009 that, according to the IRGC, were 'obscene', 'anti-religious', or 'anti-value.'[100] forty five people (mainly website managers) were arrested in 2009 as a result.[101]

After the Mozelin project, and in the wake of the 2009 election demonstrations, a new project, 'Deep Insurrection', was launched.[102] This was followed by project 'Darkoob' (Woodpecker) whose primary concern was US led espionage during these disturbances,[103] project 'Mersad' (Ambush), directed specifically against internal dissidents,[104] and project 'Foxd proj' , focused on the BBC.[105] The latest project, launched in early 2015, deals with the control of content posted on Facebook and is called 'the Spider.'[106]

[97] Shirazi, Alireza, Filtering Wave Puts Farsi Blogging in Shock, Alireza Shirazi Blog, March 2010, (online) Available at: http://shirazi.blogfa.com/post/276 Accessed: 1 March 2016.

[98] Filtering Body Performance Weakens Persian Blog Providers Status, Mihanblog, December 2010, (online) Available at: http://admin.mihanblog.com/post/186 Accessed: 1 March 2016.

[99] A Centre for Fighting Social and Cultural Corruption, Gerdab, January 2015, (online) Available at: http://gerdab.ir/fa/print/13567 Accessed: 1 March 2016.

[100] NB. the word 'value' is used for issues that the ruling regime in Iran considers in line with its interpretation of Shia Islamic values.

[101] For more information, see: http://gerdab.ir/fa/print/256 and http://gerdab.ir/fa/print/334 and http://gerdab.ir/fa/print/227 and http://gerdab.ir/fa/print/157 and http://gerdab.ir/fa/print/73

[102] Deep Insurrection in Cyberspace, Gerdab, December 2009, (online) Available at: http://gerdab.ir/fa/print/559 Accessed: 1 March 2016.

[103] Cyber Criminals, Gerdab, September 2015, (online) Available at: http://www.gerdab.ir/fa/print/15588 Accessed: 1 March 2016.

[104] Cyber Defence and National Security, Gerdab, September 2011, (online) Available at: http://www.gerdab.ir/fa/print/7360 Accessed: 1 March 2016.

[105] Details of Fox's Eye Operation, Gerdab, February 2012, (online) Available at: http://www.gerdab.ir/fa/print/9755 Accessed: March 1, 2016, . It is worth mentioning that due to the British Empire's historic involvement in the internal affairs of other countries, the UK is often referred to as the "Old Fox" in the layman's political vocabulary in Iran.

[106] New Details on the Spider Project, Gerdab, March 2015, (online) Available at: http://gerdab.ir/fa/print/13613 Accessed: 1 March 2016.

'Catphishing' and infiltration: creation of fake accounts on social media

Iranian online actors have been found to be the owners of at least 25 bogus accounts on LinkedIn, eight of which were promoted.[107] The effects of such operations can be profound, particularly in cases where targets are not sufficiently trained in online security, or provide sensitive information to the hackers under false pretences. It is feared that such attacks may only increase in complexity, making them harder to detect.

Facebook, for instance, has been the platform the authorities have most commonly used. Methods employed in order to gather information and personal data have included the following:

- Creating fake online identities to make friend requests;
- Writing provocative comments or messages to encourage responses in order to trap the target. This style of entrapment is known as an 'agent provocateur'; and
- Monitoring the public interactions of users to identify and flag trends. This includes using other group members to gather intelligence on specific individuals.[108]

Reporting social media accounts

One of the self-described 'Officers of the Cyber war' maintained a pro-ICA Facebook page, which read: "I don't know how much you know about the soft war. Soft war still has its own Facebook page, but it does not have the power it used to have two years ago. Some of the officers [members of the group] would create anti-Islamic Facebook pages and they would take the addresses offline at once at an agreed time. They would then find people who had posted anti-Islamic comments [while the pages were still up] and would report their pages to Facebook as offensive pages. Two years ago, we reported all of the people who made fun of Imam Naghi [one of the most important religious figures in Shia Islam].

The way you report a page is that you send a message to a Facebook administrator and submit a complaint that the page is offensive. If the pages reach a certain number of complaints they are then taken off Facebook and the corresponding accounts are closed. Naturally we need a large number of officers for such an operation. God willing, comrades will once again get together and make Hazrat Zahra [daughter of the Prophet Mohammad] proud by reporting the pages that are making fun of her."[109]

The complaints systems of social media sites themselves have been exploited in order to have Iranian citizens' accounts closed. In expressing potentially subversive viewpoints, unwary Facebook users are trapped by the same usage policies that are supposed to protect them from undue recrimination and exposure. This technique, though one of the less intrusive and inoffensive tactics employed, nevertheless has the ability to silence dissenting expression and impede access to social media, an increasingly vital space for the exchange of views and organisation of civil society.[110]

[107] Hacker Group Creates Network of Fake LinkedIn Profiles, Dell Secureworks, October 2015, (online) Available at: http://www.secureworks.com/cyber-threat-intelligence/threats/suspected-iran-based-hacker-group-creates-network-of-fake-linkedin-profiles/ Accessed: March 1, 2016,

[108] ARTICLE 19, Risky Online Behaviour

[109] See: https://www.facebook.com/permalink.php?story_fbid=387343911343316&id=387334654677575

[110] For instance please take a look at the following article on the Wall Street Journal on how Tavaana was a victim of such effort: http://www.wsj.com/articles/mariam-memarsadeghi-and-akbar-atri-facebook-please-dont-let-the-mullahs-troll-us-1416873076

User data gathered by companies

Iran’s authorities have tried to gain information about users directly, often from the host companies of major social networks, such as Facebook, but have thus far been unsuccessful.[111] Indeed, the only way the Iranian regime has been able to properly regulate access to Facebook has been to block its services (filter them) for extended periods of time.[112]

There was, however, some suspicion following the finalisation of the nuclear deal between Iran and the P5+1, regarding cooperation between Telegram and the Iranian Authorities, but these claims were later refuted. A few weeks after the claim, Telegram Management tweeted that the Iranian government had requested that Telegram cooperates with government agencies in spying on its users.[113] Two weeks after this claim, Telegram Management tweeted again that the previous claim was incorrect,[114] and issued this statement: “Two weeks ago Telegram stopped working in Iran, so we assumed that we had been blocked there. However, service has since returned to normal, and the Iranian Ministry of Information and Communication has declared that they were not going to permanently block Telegram.” Only a few days after this statement, the CCDOC held a meeting and decided not to block or filter Telegram.[115] Immediately after this decision, news of the incarceration of several Iranian users of Telegram was released.[116]

In a subsequent interview with Iran Wire, Pavel Durov (founder and CEO of Telegram) claimed, “We have never published or released any information regarding this or any other case.”[117] It remains unclear whether Telegram was party to the arrests, or whether any meaningful information had been shared on the accounts of those arrested.

[111] Iran Correspondences with Instagram Requesting Content Monitoring, ITNA, November 2014, (online) Available at: http://www.itna.ir/vdcfmydm.w6dmvagiiw.html Accessed: 1 March 2016.

[112] Will Viber Be Filtered in Coming Hours, Tabnak, October 2014, (online) Available at: , https://www.tabnak.ir/fa/print/443435 Accessed: 1 March 2016.

[113] Esfandiari, Golnaz and Karl Schrek, Russian Web Pioneer Says Iran Blocks Telegram App After Seeking Spying Tools, Radio Free Europe, October 2015, (online) Available at: http://www.rferl.org/content/iran-durov-russian-telegram-app-spying/27317116.html Accessed: 1 March 2016.

[114] See: https://twitter.com/durov/status/661975372116922368

[115] Meeting Outcome of Filtering Working Group: Telegram Not Filtered, Farsnews, November 2015, (online) Available at: http://www.farsnews.com/13940827001264 Accessed: 1 March 2016.

[116] See: http://www.bbc.com/persian/iran/2015/11/151118_l45_telegram_pics_arrest & and http://www.radiofarda.com/content/b33-iran-police-banned-some-telegram-chanals-arrests-100-hackers/27366836.html

[117] Telegram CEO Denies Links to Recent Arrests, Iran Wire, November 2015, (online) Available at: http://iranwire.com/features/8306/ Accessed: 1 March 2016.

Section 4
Content creation and promotion

Creating ideologically acceptable content and making sure it reaches citizens is of central importance in the Soft War: three months after the contested 2009 presidential elections, and in reaction to media coverage of the street demonstrations and the Green Movement, Khamenei declared: "the most effective international weapon against enemies and opponents is *promotion*."[118]

Content creation takes place according to three central directives. The first involves content created in order to promote and advertise a specific idea. The second focuses on content aiming to deface and discredit content created by others. Lastly, the ICA directs some resources towards upgrading and optimising previously created content. The result of these actions leads to online search engines showing content created for the ideological promotion of government-approved ideas ahead of or above unapproved content. Currently, content creation is centred on social networking websites, weblogs, and social media outlets. See Appendices 4 and 5 for more detail on content creation.

Many organisations, agencies, and corporations are indirectly involved in the Soft War. One such important organisation is Khatam al-Osia,[119] an associate of Khatam al-Anbia Construction Headquarters, which is the largest contractor working on state projects.[120] This firm is directly controlled by the IRGC and is actively involved in economic, technical, and engineering projects.[121] General Hossein Yekta, the Director of Khatam al-Osia Cultural Headquarters, believes that currently cyberspace is a battlefield, serving as preparation for a face-to-face encounter with enemies of the state.[122] Most IRGC commanders share this belief.[123]

IRGC battalions now have a large base of well-trained forces that have received different forms of advanced special training.[124] For example, Tehran's IRGC, known as Mohammad Rasul Allah Army of Revolutionary Guards of Great Tehran, have trained over 3,000 recruits throughout a one-year programme in content production. The battalion consists of specialised groups in different areas including production, audio-visual programmes, social networks, games and animation, and graphic design.[125] The battalion's objectives are to strengthen national interests, pursue the goals of the Islamic Republic within cyberspace, conduct future studies, manage messages using different languages and products, apply media-related tools, produce content in different areas, organise cyber battalions, and run cyber operations in line with the macro-level goals of the system and the Islamic Revolution.[126]

The Islamic Republic of Iran Broadcasting, or IRIB, acts as a powerful department of the Iranian state in preparing and educating Soft War forces. According to the IRIB Basij Chief, "since 2011 we have established seven cyber battalions consisting of media experts and specialists." Regarding the mission and approaches adopted by these battalions, he declared that "the IRIB Basij, as a component of the Basij Forces combats soft threats by enemies in areas such as content creation, television and radio as well as online."[127]

[118] Supreme Leader Meeting with AoE Members, Khamenei.ir, September 2009, (online) Available at: http://farsi.khamenei.ir/speech-content?id=8094 Accessed: 1 March 2016.

[119] See: http://goo.gl/1Ht57O

[120] See: http://khatam.com/ and https://en.wikipedia.org/wiki/Khatam-al_Anbiya

[121] Khatam al-Osia to Complete IRGC Dominance on Oil and Natural Gas Industry, RFI, May 2012, (online) Available at: http://goo.gl/DO8pXV ccessed: 1 March 2016.

[122] A Soft War Base Is a Necessity in the Society, Farsnews, July 2015, (online) Available at:http://www.farsnews.com/newstext.php?nn=13940506000031 ccessed: 1 March 2016.

[123] The Youth Fight the Enemies' Soft War, Dana, July 2015, (online) Available at: http://dana.ir/News/374232.html https://goo.gl/tQt6c6 ccessed: 1 March 2016.

[124] Get to Know IRGC Cyber Forces, Khabaronline, September 2015, (online) Available at:http://www.khabaronline.ir/detail/453114/Politics/military http://hizbullahcyber.com/content/25123 Accessed: 1 March 2016.

[125] Ibid.

[126] 3000 Members of IRGC Cyber Armies Attend the Military Exercise, Mehrnews, September 2015, (online) Available at: http://goo.gl/ROSv7g ccessed: 1 March 2016.

[127] Establishment of 7 Cyber Armies in the National Media, Farsnews, December 2012, (online) Available at: http://www.farsnews.com/newstext.php?nn=13910926000786 Accessed: 1 March 2016.

Basij authorities reportedly expect their members to create content in their blogs in support of the Iranian state and to post comments on other websites. Mohammad Hossein Firuz, the Secretary of the IRIB Basij Cyber Battalion Conference, stated that "seven cyber battalions are operating in political, cultural, social, and economic areas as well as media, Islamic teachings, women and family. The battalions have 1,200 active members and each battalion consists of four troops of experts in blogging and websites, social networks, mobile phones, and multimedia." In addition, "five special workgroups are responsible for supporting these battalions in monitoring, trend studies, education and planning, supply and production, security, technical issues, and infrastructural development and maintenance."[128]

Content promotion tactics

Most media managers and owners of media outlets have established parallel websites to their main news agency. There are other sources, which provide organisational and financial support for these websites.[129] These parallel websites use a complex algorithm to copy and reproduce content from the main website of the news agency, creating a multiplier effect and making government-sanctioned viewpoints widely available and pervasive for users.[130] Blanket ideological content can be desirable as it drowns out other opinions through sheer force of repetition. In general, websites employ the following strategies in the proliferation of Soft War content: reproducing content; clickjacking; promoting other websites' content; and reproducing content on blogs and social media.

1. Reproducing content – with or without citation[131]

Generally, content reproduction with citation is the accepted and common legal form for republishing news and other stories over the Internet. Most websites reprint news and stories citing the original source. Iranian media operating within Iranian cyberspace largely follow the same procedure, reproducing contents while citing sources. Stories produced by some websites are more often reproduced due to the credibility and background of these websites. News agencies like Fars, Tasnim, Al-Alam, Mashregh News, and Bultan News are among the sources that produce content on the Soft War, along with other activities related to news and media operations. Some websites, like Mashregh News, even dedicate whole pages to Soft War, indicating their focus on the topic. Common forms of reproduction often include phrases like "according to…" or "as reported by…" However, some content is reproduced without citation and copied by the outlet just to increase content volume.[132]

2. Clickjacking: using links in <iframe> tags

Inspired by online marketing strategies, <iframe> tags, used to embed another document within the current HTML document, are frequently encountered when reviewing search results: some websites contain links from a specific range of stories and content. The increasing use of this technique over the past few years can be attributed to two general aims: the first is to create websites that can help boost result counts in outputs produced by search engines; the second is to prepare websites with a

[128] National Media Cyber Armies Have More than 1200 Members, Basij, December 2012, (online) Available at: http://booshehr.basij.ir/?q=node/3298 Accessed: 1 March 2016.

[129] Media Review Analysis by independent researchers for this report.

[130] Ibid.

[131] This is part of our media review analysis. Examples are provided, http://goo.gl/QqEdCH and http://www.farsnews.com/13940527000121; http://goo.gl/Qtl47A and http://rouzegar.com/news/politics-social/t-disappearance-cream-network-host-you-and-me; and http://londoneye.blogfa.com/post/70 and http://www.yjc.ir/fa/news/4666665 and https://goo.gl/J1GwmR and http://www.mashreghnews.ir/fa/news/453471. Accessed: 1 March 2016.

[132] Iranian users tend to disregard the copyright and proper citation. However, the researchers observed that certain contents created by the websites mentioned above are heavily reproduced by other sources just to increase the traffic and volume.

large number of visitors by creating diversity and a large volume of content.[133] This also helps websites increase the number of visitors and enhance their ranks on the Alexa ranking system.[134]

3. Promoting content from other websites and providing links to original sources

Another common method for increasing traffic was employed by websites that share a large number of news links and Soft War content. A limited number of these websites have activities which are related to the subjects and topics they tag or use to describe the site, with many of them use unrelated titles like 'downloading music' and 'software' or 'cooking' and 'entertainment' to share these links. These are often referred to as 'yellow pages' which work in a similar way to Internet spamming. These websites copy content from other websites and often attract visitors by uploading images, biographies of famous people, such as actors and singers. Significantly, there are patterns which can be drawn between websites that employ these tactics: these websites have similar domain registrars or use similar techniques for development.[135]

An examination of 25 news titles published by the media reveals websites like http://vous.ir introduced as a website for 'French language, migration, jobs, and education in Quebec, and getting admission to France'. A section of this website, http://vous.ir/news/ automatically reproduces content generated by Tabnak, YJC, Bartarinha, Asr Iran, Fararu, Mashregh News, Farda News, Shafaf, Entekhab, Aftab, Serat News, Parsine, and Bultan News. Another example of a website which uses the addresses http://bestcms.in and http://tafrih.in and the title 'Net City: News, Entertainment, Couples, Fashion, Decoration, Cooking, Photos' contains the title 'Net City stories on soft war' with links that direct users to the original source.

4. Reproducing content on blogs and social media

Soft War officers play a significant role in reproducing content in blogs and social networks;[136] most of these users are conservative hardliners. Reports published in 2011 on 'Soft War officers' of this description show that they received $2.5 USD for every hour they worked on blogs and social networks for the government.[137] Assuming that a Soft War officer worked 8 to 10 hours a day, they would have received $20 to $25 USD per working day. The minimum wage of an ordinary worker was 87,840 Iranian Rials (less than $3 USD) for 8 working hours per day in 2009. Thus, Soft War officers earned almost seven times more than ordinary workers.[138]

Following such strategies, Iran was able to employ many Soft War officers in a short period,[139] who focused mostly on the following keywords: combat, fight, war, defence, attack, soft-war, sedition, conspiracy, scandal, revealing, westernisation, penetration, subversion, foreigner, anti-Islamic and anti-Iranian, satellite, BBC, Manoto, Rafio Farda, Voice of America, Wahhabi, Baha'i, Satanism, Halgheh Erfan, shrine defenders, Freemasonry, and General Soleimani. Sometimes, they provided related hashtags to categorise contents. They reproduced Soft War content and shared related links in social networks such as Google+, Twitter, Facebook, Instagram and Telegram.[140]

[133] Media Review Analysis by independent researchers for this report.

[134] This is a ranking system set by alexa.com (a subsidiary of amazon.com) that basically audits and makes public the frequency of visits on various Web sites. The algorithm according to which Alexa traffic ranking is calculated, is based on the amount of traffic recorded from users that have the Alexa toolbar installed over a period of three months. For more details, please visit: http://www.avangate.com/avangate-resources/article/alexa-ranking.htm#sthash.NxsLszVP.dpuf

[135] Media Review Analysis by independent researchers for this report

[136] Principalist Activists Receive 7000 Tomans for an Hour, Alarabiya, December 2011, (online) Available at: http://www.alarabiya.net/articles/2011/12/31/185601.html and Young Officers' Duties in Soft War, Hawzah, April 2010, http://goo.gl/fMhyoF, Accessed: 1 March 2016.

[137] Ibid.

[138] Ibid, and http://iranaccnews.com/wp-content/uploads/2014/01/2073_88.pdf?662314

[139] Job Positions in Software Team of Khuzestan Cyber Base, Afsaran.ir. May 2015, (online) Available at: http://www.afsaran.ir/link/935661

[140] Please see: http://farsi.khamenei.ir/newspart-index?tid =2748 and http://www.afsaranjnarm.ir/ and http://www.afsaran.ir/ and http://afsaran.mirzabeigi.com/ Accessed: 1 March 2016.

Section 5
Intrusive cybertactics – hacking

Introduction

Another tactic associated with potential ICA activities is intrusive computer network operations, or hacking; both campaigns of intrusion and defacement have been identified.

Equipment interference (i.e. hacking), whether carried out by a government or private actor, is perhaps the most serious form of intrusion into someone's private life, given that it involves access to private information without permission or notification. It also fundamentally breaches the integrity of the target's own security measures. Unlike search warrants, where the individual would at least be notified that their home or office was being searched, hacking generally takes place without a person's knowledge. It is the equivalent of the police breaking into someone's home. Interference with equipment can take various forms, from logging keystrokes on a computer to identifying a password with which to take control of someone's smartphone covertly, allowing photography or sound-recording without the owner's knowledge.

Since hacking is, though poorly-defined in law, illegal in Iran, and all web activities are under close scrutiny by the regime, it might be concluded that the only publicly advertised Iranian hackers are those working under the umbrella of an ICA in some form, or in line with the government's ideological goals.[141]

There appear to be three main hacking groups. The first group includes trainers and those involved in the education of other hackers. The second group handles infiltration and testing of would-be hackers. The third group comprises the main hacking group.

There have traditionally been two levels of expertise within the ICA hacking community. The first are relative amateurs who must be trained and vetted. They are mostly given simple or low-risk tasks, such as defacing and removing opposition websites. The second level is predominantly populated by professionals who attend to more sensitive and issue-specific tasks.[142]

Online attacks generally follow a common pattern. First, a target is chosen. This can be the website of an individual or an organisation. Next, the necessary level of attack (to either present a show of force, extract/steal data or intimidate) is agreed upon, and requisite research on how the actions ought to take place is completed. This step often involves an infiltration test to identify the security flaws of the target. Finally, the attack is carried out. It is assumed that another layer of key people exists in order to equip the hackers with a list of relevant issues and priorities. This list guides the actions of ICA hackers, and legitimises their actions, in that they feel they are doing something of great importance to protect the Islamic Republic of Iran.

By 2007, the IRGC had established the 'Centre for the Study of Organised Crime' (based on Article 150 of Iran's Constitution), widely considered the first Iranian government-sponsored hacking group. A few months before the 2009 Presidential election, the Fars News Agency (an organisation with alleged connections to the IRGC) stated that "ICA belongs to [the] IRGC."[143] The IRGC expanded its political and executive activities early in Ahmadinejad's second term, and began recruiting professionals for its cyber force.

[141] Rules and regulations around hacking are, however, loosely defined and vague, especially in the case of foreign hacking.

[142] Information from confidential interviews.

[143] CA Belongs to IRGC, Farsnews, May 2009, (online) Available at: http://www.farsnews.com/newstext.php?nn=8802130463 Accessed: 1 March 2016

Additionally, Basij reportedly founded the "Basij Cyber Council" in 2010 to recruit hackers to infiltrate particular websites and emails under the direct supervision of IRGC experts. In November 2010, Hossein Hamedani, Former Commander of Tehran IRGC, reported that 1,500 "cyber commandos" had been trained by the Basij Cyber Council.[144]

During the peak period of attacks on political activists' websites and email accounts of Green Movement members in March 2010, Fars News Agency published a report about a hacker who called himself a member of the ICA, a "division under the supervision of IRGC's non-executive defence forces."[145]

In a related development, the then-Intelligence Minister, Heidar Moslehi, stated in an interview with IRIB that "outlets have confessed that the ICA has been able to halt their activities and prevent their conspiracies."[146] Two days prior to the interview with Moslehi, the Islamic Republic of Iran News Agency (IRNA) announced that "the Americans had several projects to challenge the security of the Islamic Regime's cyberspace, but the security forces prevented these attacks and have neutralised the American plot. Even some Western media outlets and websites have admitted that the ICA has stopped the schemes of the West."[147]

Official declarations aside, there appears to exist a network of governmental science centres or independent hacking groups, which enjoy immunity and support from the Iranian authorities. In the last few years, most state-owned universities and several of the nation's most prominent scientific centres have established professional CERT Centres as well as research, development, and educational laboratories specifically focused on hacking and cyber security. Of particular note is the University of Imam Hossein, which is owned and operated by the IRGC.[148] In addition, Sharif Industrial University holds training courses, teaching hacking techniques to university students. Sharif Industrial University is one of Iran's top scientific and industrial universities, ranked between 471 and 480 of the top universities in the world.[149] The universities may tacitly provide support and training for assets that could be associated with Iran's cyber security strategy.

Hacking groups

The secretary of the E-Government Conference has specifically praised the group 'Ashiyane' (Nest) for its role in the events following the 2009 presidential elections, and invited the Group to discuss its experiences regarding Cyber Safety, and draw on its broad experience in fighting against "immoral websites and the online actions of the Zionist Entity."[150]

[144] Basij Trains 1500 Cyber Commandos, Tabnak, November 2010, (online) Available at: https://goo.gl/zdII6X AAccessed: 1 March 2016. Cyber Armies Mobilized in the National Media, pririb.ir, November 2014, (online) Available at: http://www.pririb.ir/persian/ModulesPage.aspx?modulename=news2&action=viewtext&news=42569 and Open Letter Released by Student Basij Office of Alborz Universities, Basijnews, October 2015, (online) Available at: http://goo.gl/CNTbOZ Accessed: 1 March 2016.

[145] ICA from A to Z, Farsnews, February 2010, (online) Available at: http://www.farsnews.com/printable.php?nn=8812040390 Accessed: 1 March 2016.

[146] MOI Achievements in 2010/2011, Mashreghnews, March 2011, (online) Available at: http://www.mashreghnews.ir/fa/print/35659 Accessed: 1 March 2016.

[147] Americans Are Aware of Their Own Defeat, Mashreghnews, March 2011, (online) Available at: http://www.mashreghnews.ir/fa/print/35425 Accessed: 1 March 2016.

[148] Who Is the Target of New US Sanctions?, BBC, November 2012, (online) Available at: http://www.bbc.com/persian/iran/2012/11/121109_mgh_iran_us_treasury_sanctions.shtml Accessed: 1 March 2016.

[149] See: http://www.topuniversities.com/universities/sharif-university-technology

[150] Third Conference on e-Government Security, ITNA, October 2009, (online) Available at: http://www.itna.ir/vdchkznz.23nxwdftt2.html Accessed: 1 March 2016.

Ashiyane was also invited to an official seminar in the city of Qom to teach email hacking, infiltration of Linux servers, DDoS, and SQL Injection techniques.[151] In its 13 years of activity, Ashiyane has been praised by numerous entities such as the Grand Ayatollah Makarem Shirazi (a Shiite religious authority) for hacking into Wahabi websites;[152] the Islamic Republic of Iran's Army; FATA Police, and various divisions of the IRGC.[153]

With 363,949 members, the Ashiyane group is the largest hacker-training forum in Iran. In January 2011, it enrolled 460 online members at one time, which constituted the largest number of online participants at any given time in Iranian history. On average, there are 30 people enrolled in online courses at any one time. In 2009, during the peak of cyber attacks against government opposition websites, Ashiyane released an instructional package for hacking.[154] This package (based on this image capture)[155] is not being offered anymore, at the request of FATA forces. The package listed the following in its syllabus:

- Hacking Linux and Windows based servers;
- Different methods of hacking;
- Hacking methods, training articles, and books in Farsi and English;
- Selected courses from Ashiyane Group's community server;
- "Infiltration level tests" for net and site managers; and
- Ashiyane-specific tools for security breaches and hacking.

The name of their training package was eventually changed to 'Security and Counter-Infiltration.'[156] However, the titles of the educational package clearly show that the main purpose of the course is hacking and not just increasing security. Ashiyane seem to have found creative ways to offer their services through other channels to maintain their immunity. Examining the contents of the programme, it is clear that, with the exception of several introductory points (see Appendix 7), all other lessons are focused on hacking. Initially, the main instructors at Ashiyane (namely, Behrooz Kamalian and Nima Salehi) set up several courses entitled 'Hacking and Security' at Sharif Industrial University.[157] However, based on an agreement signed between the university and Ashiyane in October 2015, Sharif University has now developed its own dedicated 'Security and Counter-infiltration' programme, and issues its own certificates for students.[158] Details of this programme are available in Appendix 7.

In addition to its links to the IRGC, it appears that the Ashiyane Group has some level of cooperation with the FATA Police. On October 2015, a Legal Assistant to FATA Police announced, "Based on Islamic Penal Law articles 725 and 753 (sections A, B and C), hacking, infiltration and unauthorised access to data and the sales of hacker training software or training packages can be considered a criminal offense. FATA will confront hackers and site owners who promote hacking or provide access to hacking software."[159] Interesting to note is the fact that some of the main hacking groups (including Ashiyane) seem not to have been subjected to the new FATA laws.

[151] Ashiyane Group Attends Counter-Infiltration Seminar in Qom, Ashiyane, (online) Available at:, http://goo.gl/0yWDOI Accessed: 1 March 2016.

[152] See: http://www.ashiyane.ir/News/ashiyane.jpg

[153] The document is a private picture of one our sources taken from Behrooz Kamalian (of the award and appreciation plaque) that cannot be published due to security purposes.

[154] The Instructional Package "Shekaf", Ashiyane, (online) Available at: http://goo.gl/exy14S, Accessed: March 1, 2016,

[155] Please see: https://goo.gl/btFV7U

[156] Security and Counter-Infiltration Methods, Ashiyane, (online) Available at: http://train.ashiyane.ir/security/ Accessed: 1 March 2016.

[157] Security Workshop in Sharif University, Ashiyane, (online) Available at: http://goo.gl/AcXC9b and http://goo.gl/8M3GDB Accessed: 1 March 2016.

[158] First Exam in Sharif University IT Centre, Ashiyane, (online) Available at: http://goo.gl/sKHFj6 Accessed: 1 March 2016.

[159] Nationwide Operation to Identify Hackers, Fardanews, October 2015, (online) Available at: http://www.fardanews.com/fa/print/455980, Accessed: 1 March 2016.

A former member of the Ashiyane Group[160] stated that Behrooz Kamalian is actually a member of the FATA Police, and has described how Kamalian captured several people while conducting a police operation.[161] This was eventually admitted by Kamalian himself in an interview published on 1 July 2015 by Afsaran, a website dedicated to ICA hackers.[162] While the Ashiyane group is mainly concerned with the pedagogical elements of hacking, it has also engaged in hacking activities itself. Based on rankings provided by zone-h.org, the Ashiyane group is ranked second in on a global list of defacing websites (hacking and altering content on the first page of a website).[163] On his Instagram page, Behrooz Kamalian has boasted that nearly 72,000 of the websites his team have hacked have been foreign governmental websites (as opposed to websites owned by individuals).[164]

Multiple other groups have been identified as active hacking groups with some connection to an ICA entity (see Appendix 2 for more) Gerdab Group, Shabgard Group, Black Hat Group, Vampire Group, Iran Hack, Hezbollah Cyber Army, and the Iranian Dark Coder Team. Guarnieri and Anderson, in their ongoing research into the Iranian Soft War online, have identified a number of other campaigns and groups, including Rocket Kitten, Infy, Sima, and Cleaver (Ghambar).[165]

Cyber Army: a profile of recruits

Members of hacking groups tend to share four main profile criteria.[166] They are generally young, largely in their early twenties, and eager to start a family at an early age (in line with the religious guidelines of the ruling classes). They often use images of religious figures in their social media activities and masked photos of themselves on their online profiles, or wear military fatigues in pictures posted on social media, and engage in promotion, glorification, and tribute to IRGC's top commanders (in particular, General Soleimani), the Supreme Leader of Iran, and the regime's allies (such as Russia, Syria, Lebanese armed-group Hezbollah, and the Yemeni Houthis).[167]

Though no employment structures or salaries as such have been identified, Guarnieri and Anderson identified that actors seem to be working in times which correspond with working hours: *"At the most basic level, the groups of actors follow similar patterns of life approximating that of an Iranian workday (Saturday through Wednesday) and are fully dormant on Iranian holidays, particularly the long vacation period of Nowruz."*[168]

[160] This is also reconfirmed in a couple of other interviews the researchers conducted with other former members of AshTiyane, or groups close to Ashiyane. Article 19 cannot verify this.

[161] Interview with former Ashiyane member.

[162] Interviews with other former members of Ashiyane

[163] See: http://www.zone-h.org/archive/notifier=Ashiyane%20Digital%20Security%20Team?zh=1

[164] Behrooz Kamalian Instagram Page (Public), (online) Available at: , https://www.instagram.com/p/4uiAR-RHmR/ Accessed: 1 March 2016.

[165] Guarnieri & Anderson, ibid.

[166] See Methodology for information on sources.

[167] Several illustrations of these markers and the underlying characteristics of the hackers are documented by ARTICLE 19. Observations are drawn through interviews conducted with members of Ashiyane amongst other groups, as well as screening the social media profiles of identified members. There are few evidences publicly available on characteristics of these individuals. Hamshahri has conducted an interview with a few members of Ashiyane group which further testifies on the authenticity of our observations: http://www.ashiyane.ir/News/ashiyane.jpg.

[168] Guarnieri Anderson, ibid, p3.

Hacking techniques[169]

Remote Access Technology or Remote Administration Technology (RAT)

The increasing popularity of Android systems in the Middle East (around 80% of phone owners operate Android devices) has led to a trend among Iranian hackers for Android RATs: a tool that facilitates remote spying on Android mobile phones. Research conducted for this study in 2015 supports this trend.[170] This preference is seen not only among Iranian hackers but also within many hacking communities in the region. For instance, during the attack in Paris on the French magazine *Charlie Hebdo* in January 2015, non-Iranian hackers used #JeSuisCharlie to spread malware via the DarkComet RAT, based on the Android operating system.[171]

Phishing

Combined with social engineering techniques, phishing can be highly dangerous, posing serious risks to the freedom and anonymity of Internet users, particularly in regions where such information can be misused by government forces. Impersonation Facebook accounts and email addresses, particularly relating to human rights organisations and political groups, have been used to gain access to devices and other account data, enabling surveillance and monitoring of individuals.

A study of security teams in Iran shows that certain hacks carried out via phishing attacks were designed for specific targets. If the target uses Second-Step Verification, then hacking is done using a more complex method, usually by putting time pressure on the target.[172]

Spear phishing is a more targeted form of phishing, using emails designed to appear to be from a trusted or known sender, often using a subject line or content tailored to the target's interests or profession. Attackers may even study the target's Facebook, LinkedIn and other social media accounts to ascertain the names of trusted people in their circle or impersonate or a topic of interest.

Spear phishing tactics have been used in Iran to gain access to social media and email accounts, the 'Rocket Kitten' group breached the accounts of a prominent Iranian in April 2016, then began to communicate with her contacts and individuals in the human rights community, attempting to gain access in turn to their Telegram messaging accounts. These tactics appear to have been used in Iran in order to gain access to the Telegram accounts of multiple individuals connected with political opposition figures, women's rights activists and other surveillance targets.[173]

[169] See Methodology: this list strives to be as comprehensive as possible, but the findings are limited by the scope and range of sensitive information accessible through primary source analysis and interview techniques.

[170] Iranian Hackers' Rising Interest in Targeting Android Systems With DroidJack, AndroRAT, Recorded Future, (online) Available at: https://www.recordedfuture.com/iranian-forums- targeting-android/ and Villeneuve, Nart et al, Operation Saffron Rose, Fire Eye, May 2014, (online) Available at: https://www.fireeye.com/blog/threat-research/2014/05/operation-saffron- rose.html All accessed: 1 March 2016.

[171] #JeSuisCharlie Movement Leveraged to Distribute DarkComet Malware, Recorded Future, January 2015, (online) Available at: https://www.recordedfuture.com/darkcomet-malware-analysis/ Accessed: 1 March 2016.

[172] Citizen Lab, London Calling: Two-Factor Authentication Phishing From Iran, 27 August 2015, https://citizenlab.org/2015/08/iran_two_factor_phishing/

[173] Guarnieri & Anderson, ibid, pp29-30.

Messages claiming to be sent from the Emergencies Director of Human Rights Watch in February 2016, referencing a genuine Human Rights Watch report, directed users to malware-tainted documents via hyperlinks seemingly to the Director's biography and article.[174]

DDoS Attacks[175]

In 2012, Iranian hackers repeatedly attacked Bank of America Corp. (BA.N), JPMorgan Chase & Co. (JPM.N) and Citigroup Inc. (C.N), reportedly as part of a broad cyber campaign targeting the US.[176] Balatarin is an Iranian website, hosted abroad, which was also the victim of this technique.[177]

The Effects of Hacking

Though it is difficult to measure the effectiveness or outcome of these tactics overall, it is certain that huge resources are being invested in this online activity, both intrusion and defacement campaigns, and that a large number of individuals are involved. A secondary effect of this large-scale and well-publicised hacking is the creation of an atmosphere of fear online, causing a 'chilling effect' in activities and communications, which cannot be guaranteed to be secure and therefore pose a risk of being read or monitored, leading to arrest or harassment.

Then Intelligence Minister, Heidar Moslehi, stated in an interview with IRIB that "some media outlets have confessed that the ICA has been able to halt their activities and prevent their conspiracies."[178] Two days prior to the interview with Moslehi, the Islamic Republic of Iran News Agency (IRNA) announced that "the Americans had several projects to challenge the security of the Islamic Regime's cyberspace, but the security forces prevented these attacks and have neutralised the American plot. Even some Western media outlets and websites have admitted that the ICA has stopped the activities of the West."[179]

The clearest evidence of IRGC involvement in hacking came from a report published by the Entekhab News Agency in December 2013, which reported that nine opposition websites had been hacked by "the Cyber Forces of IRGC's intelligent units of the Kermans' Sarallah's Brigades."[180] Seemingly, after a period of denial between 2011 and 2013, the government had begun to announce proudly the successes of this new unit.

When hackers themselves are targeted, they are often subsequently recruited to work for the agenda of the authorities. Hackers are usually classified as either black – or white – hat hackers. Criminal hackers (black-hat hackers)

[174] Guarnieri & Anderson, ibid, p37.

[175] A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information. For more information, please visit: http://www.digitalattackmap.com/understanding-ddos/

[176] Finkle, Jim, and Rick Rothacker, Exclusive: Iranian hackers target Bank of America, JPMorgan, Citi September 2012, (online) Available at: http://reut.rs/QqivK2 Accessed: March 1, 2016 177 Google wants to save ews sites from cyberattacks, https://www.wired.com/2016/02/google-wants-save-news-sites-cyberattacks-free/

[177] MOI Achievements in 2010/2011, Mashreghnews, March 2011, (online) Available at: http://www.mashreghnews.ir/fa/print/35659 Accessed: 1 March 2016.

[178] Americans Are Aware of Their Own Defeat, Mashreghnews, March 2011, (online) Available at: http://www.mashreghnews.ir/fa/print/35425 Accessed: 1 March 2016.

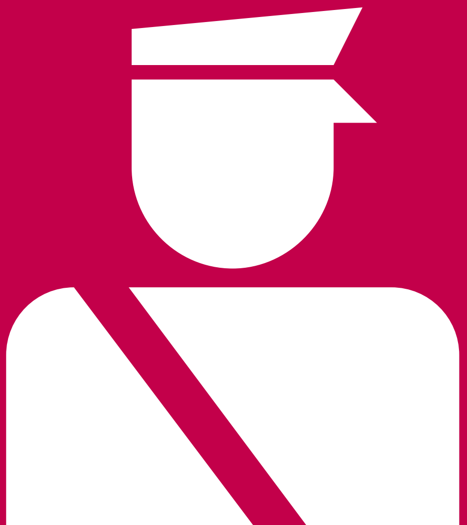
[179] Americans Are Aware of Their Own Defeat, Mashreghnews, March 2011, (online) Available at: http://www.mashreghnews.ir/fa/print/35425 Accessed: 1 March 2016.

[180] IRGC Cyber Forces Hack 9 Dissent Websites, Entekhab, December 2013, (online) Available at: http://www.entekhab.ir/fa/print/142066 Accessed: 1 March 2016.

have already spent time in prison. Many black-hat hackers are induced or coerced into working for the government. Professional hackers (white-hat hackers) do not have a criminal record, but are nonetheless put under pressure to work for the government agenda.[181]

[181] ARTICLE 19, Report: Computer Crimes in Iran – Risky Online Behaviour.

Section 6 International human rights



The Right to Freedom of Expression and Information

Freedom of expression and information is a fundamental human right. The full enjoyment of this right is central to achieving individual freedoms and to developing democracy, as demonstrated by the ongoing democratic transitions occurring in several of Iran's near neighbours. Freedom of expression is a necessary condition for the realisation of the principles of transparency and accountability that are, in turn, essential for the promotion and protection of all human rights.

The International Covenant on Civil and Political Rights (ICCPR) elaborates upon and gives legal force to many of the rights articulated in the Universal Declaration of Human Rights: it binds its 167 state parties to respect its provisions and implement its framework at the national level.[182]

Article 19 of the ICCPR guarantees the right to freedom of expression as follows:

Everyone shall have the right to freedom of opinion

Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art or through any other media of his choice.

Iran signed the ICCPR on 4 April 1968 and ratified it on the 24 June 1974: Iran is thus legally bound to respect and ensure the right to freedom of expression as contained in Article 19.

While Article 19 is a fundamental right, it is not guaranteed in absolute terms. However, it can only be restricted subject to three strict conditions enunciated in Article 19 (3) ICCPR. In particular, restrictions must:

- Be provided by law;[183]
- Pursue one or more of the legitimate aims exhaustively listed under Article 19 (3), namely respect for the rights or reputations of others, the protection of national security or public order, public health or morals; and
- Be strictly necessary and proportionate in a democratic society. Importantly, restrictions on the right to freedom of expression must be interpreted and applied strictly and narrowly.

The same principles apply to electronic forms of communication or expression disseminated over the Internet: the HR Committee has said in its General Comment No. 34 that:

> "Any restrictions on the operation of websites, blogs or any other Internet-based, electronic or other such information dissemination system, including systems to support such communication, such as Internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3. It is also inconsistent with paragraph 3 to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government."[184]

In September 2011, the UN Human Rights Committee (HR Committee), the UN treaty-monitoring body, expressly recognised that Article 19 of the ICCPR protects all forms of expression and the means of their dissemination, including all forms of electronic and Internet-based modes of expression.[185]

In addition, General Comment No. 34 calls on state parties to take all necessary steps to foster the independence of new media and ensure access to them, and 2016's UN HRC Resolution on 'the promotion, protection and enjoyment of human rights on the Internet' (A/HRC/32/L.20) further commits states to:

Address security concerns on the Internet in accordance with their obligations to protect freedom of expression, privacy and other human rights online;

Desist and refrain from "measures to intentionally prevent or disrupt access to or dissemination of information online". This includes measures to shut down the Internet or part of the Internet at any time, in particular at times where access to information is critical, such as during an election, or in the aftermath of a terrorist attack; and

Adopt a "human rights based approach" to provide and expand access to the Internet.[186]

Clearly, these standards are not being upheld in Iran, where authorities are not only restricting the Internet usage of their citizens, but using the online sphere as a place to monitor and restrict the flow of information.

Content Restriction: Blocking and Filtering

Article 19 (1) of the ICCPR provides that the right to freedom of expression includes the individual's freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers and through any other media of his choice.

Filtering and blocking interfere with the right to seek and exchange information and ideas: filtering and blocking technologies are blunt instruments, which tend to over-block or under-block content, with the result that legitimate content may be unduly restricted. Website blocking can only be compatible with international standards on freedom of expression in cases where it has been provided by law and a court has determined that a blocking measure is necessary in order to protect the rights of others, or in the case of filtering, where it has been voluntarily adopted by the individual user.

Blocking measures must always comply with the three-part test under Article 19(3) ICCPR:[187] they must be provided by law, proportionate, and necessary. There are specific criteria which must be met in order for website blocking and filtering to be justified under international law:

1. Blocking and filtering provisions should be clearly laid out by law;[188]

2. Any determination on what content should be blocked must be undertaken by a competent judicial authority or a body which is independent of any political, commercial, or other unwarranted influences;

3. Blocking orders must be strictly limited in scope in line with the requirements of necessity and proportionality under Article 19 (3);

4. Lists of blocked websites together with full details regarding the necessity and justification for blocking each individual website should be published.

5. An explanation should also be provided on the affected websites as to why they have been blocked.

The total lack of transparency around Iran's blocking and filtering programme, as well as the clear politicisation of the criteria, demonstrate a manifest disregard for these standards.

[182] Article 2 of the ICCPR, GA res. 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 52, UN Doc. A/6316 (1966); 999 UNTS 171; 6 ILM 368 (1967).

[183] General Comment No 34 provides the following clarification that "Since any restriction on freedom of expression constitutes a serious curtailment of human rights, it is not compatible with the Covenant for a restriction to be enshrined in traditional, religious or other such customary law." General Comment No. 34, CCPR/C/GC/34, adopted on 12 September 2011, para.24 piuur.html

[184] General Comment No. 34, CCPR/C/GC/34, adopted on 12 September 2011, para. 43.

[185] Ibid. para 12.

[186] Resolution A/HRC/32/L.20 https://www.article19.org/data/files/Internet_Statement_Adopted.pdf ; see also ARTICLE 19's statement on the passing of the resolution: https://www.article19.org/resources.php/resource/38429/en/unhrc:-significant-resolution-reaffirming-human-rights-online-adopted

[187] Ibid. para 81.

[188] Ibid.

Surveillance of communicators and activists

Privacy is a fundamental human right, and is essential to human dignity. It reinforces other rights including the right to freedom of expression and information, and freedom of association, and is recognised under international human rights law.[189] Communications surveillance interferes with the right to privacy among a number of other human rights. As a result, it may only be justified when it is prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.[190]

The 2013 report of the UN Special Rapporteur on freedom of expression highlighted the important relationship between the rights to privacy and freedom of expression in cyberspace.[191] The report also observed that restrictions to anonymity facilitate states' communications surveillance and have a chilling effect on the free expression of information and ideas.[192] David Kaye, current UN Special Rapporteur on freedom of expression, in his 2015 Report, observed that restrictions on anonymity, and communications surveillance, have a chilling effect on the free expression of information and ideas.[193]

Hacking

ARTICLE 19 believes that the use of hacking by, or sanctioned by, government officials is, in general, a clear violation of the rights to privacy and free expression, given that it involves access to private information without permission or notification, and is in breach of the integrity of the target's own security measures. Unlike search warrants where the individual would at least be notified that their home or office was being searched, hacking generally takes place without a person's knowledge. It is the equivalent of the police breaking into someone's home.

Given the obvious intrusiveness of such a measure, it should only be authorised by a judge in the most exceptional circumstances and must be subject to strict conditions. In particular, hacking should only be available for the most serious offences and as a last resort, once other, less intrusive methods have already been exhausted.[194]

The chilling effect

Vague laws with harsh penalties, combined with the total lack of transparency around online regulation and how expression might be monitored, regulated, or punished, and lack of knowledge, are likely to have a strong chilling effect on the online behaviour of activists and normal citizens, meaning that many will self-censor out of fear is a serious threat to free expression and the free flow of information.

[189] Universal Declaration of Human Rights Article 12, International Covenant on Civil and Political Rights, International Covenant on Civil and Political Rights Article 17

[190] See also Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance, 2014, developed by ARTICLE 19 as part of a coalition of privacy and human rights organisations; available here https://necessaryandproportionate.org/principles

[191] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/23/40, 17 April 2013 (the 2013 Report of the SR on FOE), para 47.

[192] Ibid para 48-49.

[193] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/23/40, 17 April 2013 (the 2013 Report of the SR on FOE), paras 48-49.

[194] ARTICLE 19, The Right to Anonymity, 2015, https://www.article19.org/resources.php/resource/38006/en/report:-the-right-to-online-anonymity

Conclusions

Iran has always feared unrestricted access to information via the Internet. The country has a track record of online censorship through Iranian authorities, security services, and even grassroots cyber-activists: an approach typified by intimidation and the desire to silence activists, journalists, human rights defenders and those that dissent through constant online attacks.

While online actors and groups have remained secretive about their structure and direct links to Iranian security and military establishments, it is clear that they enjoy a great amount of support and legal immunity in their work. Activities and priorities also appear to be directly in line with Khamenei's Soft War rhetoric, which they adhere to via mass creation of content and targeting political opposition voices online.

The role and effect of the ICA cannot be underestimated. With its dedicated taskforce and a broad institutional support, this organisation has harnessed the influence and power of the IRGC to engage in both offensive and defensive censorship of the Internet in Iran, as well as using the Internet to monitor and persecute civil society. It is clear that the ICA has been successful in having a chilling effect on freedom of speech online. Iranian authorities have also publicised their work with the aim of creating further fear among Internet users in Iran.

Recommendations

Recommendations to the authorities of the Islamic Republic of Iran

The Government of the Islamic Republic of Iran should:

- Stop the blocking and filtering of all online content under the justification of the 'Soft War'. Any content filtering by the government or commercial service providers which is not end-user controlled is a form of prior censorship, and is not justifiable as a restriction on freedom of expression;
- Respect the online privacy and anonymity of its people and immediately stop subjecting them to unlawful surveillance. All surveillance must be in accordance with Article 17 of the International Covenant on Civil and Political Rights. Mass surveillance (or 'bulk collection') is an inherently disproportionate interference with human rights, and the Islamic Republic of Iran must ensure it complies with international human rights standards in this regard;
- Repeal the Computer Crimes Law in its entirety, and enact comprehensive legal reform to permit the full exercise of freedom of expression;
- Immediately withdraw any official support or backing from any individual, network, or group engaging in hacking or online attacks; and
- Immediately end any legal immunity that an Iranian Cyber Army network might enjoy in monitoring, online attacks and hacking;

The IRGC and other military and security organisations must immediately withdraw their support for networks engaging in hacking or other abuses of human rights online.

The IRGC must respect Iranian citizens' right to free expression and privacy, and therefore must end the intimidation campaign highlighted by Soft War rhetoric.

Recommendations to the Iranian online community

The online community in Iran must be vigilant and aware of state-controlled threats such as surveillance, identity theft, hacking, phishing, content blocking and filtering.

For a detailed set of recommendations to the online community in Iran, please see ARTICLE 19's report *Computer Crimes in Iran: Risky Online Behaviour.*[195]

[195] Computer Crimes Iran: Risky Online Behaviour, 2013 https://www.article19.org/data/files/medialibrary/38039/Risky-Online-Behaviour--final-English.pdf Accessed: 1 March 2016.

Methodology

This report examines the origins and activities of a collective force and the strongest component of Khamenei's Soft War strategy, which has been referred to as a potential Iranian Cyber Army (ICA) throughout this report, though, as discussed above, the exact boundaries, organisation, and support of this network of actors and individuals remains unclear. The report's analysis will shed light on the implications of the network's activities and suggest ways in which their negative effects on freedom of expression online could be minimised.

The findings and recommendations of this report are based on ARTICLE 19's core values in protecting freedom of expression and information. In order to paint a comprehensive picture of activities associated with the Soft War, this report has considered, analysed, and documented some of the effects of the network of actors' activities on the human rights of Iranian Internet users.

The data collected and analysed for this report is comprised of extensive surveys of primary and secondary source materials related to the Soft War. As primary sources, the team of researchers interviewed 15 individuals, aged 17 to 35, the majority of them aged 18–22, 14 males and 1 female, and from geographically diverse places. All interviewees have at some point been part of a hacking operation, ranging from defacement to data exploitation. Not all interviews are in a voice recorded format, some being in chat formats collected through various means. The team of researchers also joined three private hacking groups and dozens of public groups to monitor trends and hackers' social habits.

All figures within the report have been cross-checked and validated to ensure their validity and to meet high standards of research integrity. Such an endeavour has nonetheless met with challenges, especially given the fact that access to objective information is often restricted in Iran. However, the information used in this report was verified by sources both inside and outside of Iran prior to its publication.

Data used in this report was collected between September and December 2015. While statements released after this date will not be analysed as part of this report, no development after March 2016 has suggested a change in finding and analysis of this report, and therefore the findings of this report remain relevant and highlight the threat to the freedom of expression and access to information posed on the citizens of Iran.

The report does not look into Iran's defensive Soft War strategy or activities protecting itself against attacks from other states and entities.

The exchange rate used is 1 USD:3000 Tomans
(1 Toman:10 Rials)

Appendices

Censorship Systems	
Jan 2005	Researchers claimed that Iran employs a package called Smart Filter, developed by the US company Secure Computing. However, Secure Computing informed the *New Scientist* that Iran's state-controlled ISPs are using the company's software without permission: "Secure Computing has sold no licenses to any entity in Iran", claims spokesman David Burt. "We have been made aware of ISPs in Iran making illegal and unauthorized attempts to use our software".[196]
Oct 2006	Service providers were told to restrict online speeds to 128 kilobits per second (kbps) and were forbidden from offering fast broadband packages. [197]
Dec 2014	Intelligent censorship: ICT Minister Mahmoud Vaezi declared that an intelligent filtering programme had entered its pilot phase, blocking immoral and criminal content. Iran's cyber police, Gerdab, however stated that the intelligent filtering programme was not functional on websites that use the SSL protocol. [198]

Appendix 1: Timeline of Key ICA-Related Techniques and Events

Censorship Systems	
Jan 2011	SSL-based communications were restricted to 2 kilobit per second rates or simply blocked altogether.[199]
Sep 2011	Port Blocking: After the Iranian election and the Arab awakening movements that were fuelled to some extent by social media, the Iranian government began to block all social websites, including Facebook, Youtube, Orkut, MySpace, and Twitter. Iranian citizens, however, started using VPN (virtual private network) connections to bypass censorship. However, after Thursday, 30 September 2011, all VPN ports were blocked in the first attempt to start what the Iranian government calls the 'National Internet'.[200]
Sep 2012	The government improved its efforts to block Tor network access. Tor attempts to disguise its traffic like a web browser communicating with an https web server, although closer inspection can yield some differences. In this case, the characteristic of Tor's SSL handshake were examined by the government, particularly, the expiry time for our SSL session certificates: Tor rotates the session certificates every two hours, whereas normal SSL certificates typically last a year or more. The fix was to simply write a longer expiration time on the certificates, so as to produce more plausible expiry times.[201]
2/1/2012	Iran started to filter SSL connections on much of their network.[202]

[196] https://www.newscientist.com/article/dn7589-iranian-net-censorship-powered-by-us-technology/ Accessed: 1 March 2016.

[197] http://www.theguardian.com/technology/2006/oct/18/news.iran Accessed: 1 March 2016.

[198] https://advox.globalvoices.org/2015/05/07/new-research-iran-is-using-intelligent-censorship-on-instagram Accessed: 1 March 2016.

[199] https://blog.torproject.org/blog/new-blocking-activity-iran Accessed: 1 March 2016.

[200] https://gist.github.com/collina/5521087 & http://yro.slashdot.org/story/11/10/06/1328211/Iran-Blocks-VPN-Ports?utm_source=rss1.0moreanon&utm_medium=feed Accessed: 1 March 2016.

[201] https://blog.torproject.org/blog/iran-blocks-tor-tor-releases-same-day-fix Accessed: 1 March 2016.

[202] https://archive.torproject.org/monthly-report-archive/2012-February-Monthly-Report.pdf Accessed: 1 March 2016.

Corrupted Software

May 2012	CitizanLab reported that software was being recommended and circulated among Syrian Internet users for bypassing censorship in their country, which led to the discovery and analysis of a back-doored version of this software. The malicious copy installs the Simurgh software, but also installs an undesirable backdoor on the victim's computer. This software is distributed as "Simurgh-setup.zip" and is identifiable via the md5 and sha256 hashes.[203]

Hacking

May 2015	The Wall Street Journal reported that: "Iranian hackers were able to gain access to control-system software that could allow them to manipulate oil or gas pipelines. … The developments show that while Chinese hackers pose widespread intellectual property theft and espionage concerns, the Iranian assaults have emerged as far more worrisome because of their apparent hostile intent and potential for damage or sabotage".[204]
Dec 2011	Decrypting RSA: "Researchers from ETH Zurich in Switzerland, and UCI Irvine in the United States released a paper in which they reveal the results of experiments done with the purpose of simulating a Global Positioning System (GPS) attack, similar to the one allegedly used by Iran to capture an RQ-170 warplane".[205]
Jul 2011	Man in the Middle (MITN) Attacks: "More facts have recently come to light regarding the compromise of the DigiNotar Certificate Authority, which appears to have enabled Iranian hackers to launch successful man-in-the-middle attacks against hundreds of thousands of Internet users inside and outside of Iran."[206] "The tally of digital certificates stolen from a Dutch company in July has risen to more than 500, including ones for intelligence services like the CIA, the U.K.'s MI6 and Israel's Mossad, according to a Mozilla developer".[207]
Aug 2015	Phishing: phishing phone calling schemes "were detailed in an August 2015 report by Citizen Lab, describing attempts to lure victims to provide their two-factor authentication tokens. In these attempts, victims receive tailored calls from a person who has clearly researched them, prompting them to take action on received emails. Among targeted victims Citizen Lab mention EFF's Director for International Freedom of Speech Jillian York. The Citizen Lab report describes overlapping phishing domains with ones previously reported, confirming a link with Rocket Kitten."[208]

[203] https://citizenlab.org/2012/05/iranian-anti-censorship-software-simurgh-circulated-with-malicious-backdoor-2 Accessed: 1 March 2016.

[204] https://wikileaks.org/hackingteam/emails/emailid/55246 & http://www.wsj.com/articles/SB10001424127887323336104578501601108021968 Accessed: 1 March 2016.

[205] http://news.softpedia.com/news/Experts-Question-Iranian-GPS-Attack-to-Capture-Drone-242310.shtml & https://cryptome.wikileaks.org/0005/iran-rsa-cipher.htm Accessed: 1 March 2016.

[206] https://www.eff.org/deeplinks/2011/09/post-mortem-iranian-diginotar-attack Accessed: 1 March 2016.

[207] http://www.computerworld.com/article/2510950/security0/hackers-steal-ssl-certificates-for-cia--mi6--mossad.html Accessed: 1 March 2016.

[208] http://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf Accessed: 1 March 2016.

May 2014	Social Engineering (targeting individuals holding key roles): Iranian actors are using more than a dozen fake personas on social networking sites (Facebook, Twitter, LinkedIn, Google+, YouTube, Blogger) in a coordinated, long-term cyber espionage campaign. At least 2,000 people are, or have been, caught in the snare and are connected to the false personas.[209]
May 2014	Social Engineering (Targeting key actors): The Wall Street Journal reported that: "Hackers apparently based in Iran mounted a three-year campaign of cyber espionage against high-ranking U.S. and international officials, including a four-star admiral, to gather intelligence on economic sanctions, antinuclear proliferation efforts and other issues, according to cybersecurity investigators."[210]

Malware

Feb 2015	"The GHOLE malware campaign involves victims being sent spear phishing emails with malicious attachments. The attachment is usually an Excel file that contains a malicious macro. When clicked, the Excel file drops a .DLL file that will then be executed by the malicious macro embedded in the Excel file."[211]
Feb 2015	Operation Woolen-GoldFish: Operation Woolen Goldfish involves spear phishing emails embedded with a malicious link that leads to a OneDrive link. The link goes directly to a malicious file download. The malware payload was initially found to be a variant of GHOLE, but further samples led to the discovery of a new payload: a variant of a keylogger known as the CWoolger keylogger. It is detected as "TSPY_WOOLERG.A".[212]

Surveillance Systems

Apr 2009	It was reported that last year, "Nokia Siemens Networks (NSN), a joint venture between the Finnish cell-phone giant Nokia and German powerhouse Siemens, delivered what is known as a monitoring center to Irantelecom, Iran's state-owned telephone company. A spokesman for Nokia Siemens Networks said the servers were sold for 'lawful intercept functionality,' a technical term used by the cell-phone industry to refer to law enforcement's ability to tap phones, read e-mails and access electronic data on communications networks."[213]
Mar 2012	"A Chinese telecommunications equipment company sold Iran's largest telecom firm a powerful surveillance system capable of monitoring landline, mobile and Internet communications, interviews and contract documents show."[214]
Jun 2011	"China's ZTE Corp, which recently sold Iran's largest telecommunications firm a powerful surveillance system, agreed to ship to Iran millions of dollars worth of embargoed U.S. computer equipment, documents show."[215]

[209] http://www.isightpartners.com/2014/05/newscaster-iranian-threat-inside-social-media/ Accessed: 1 March 2016.

[210] http://www.wsj.com/articles/iran-based-cyberspies-targeting-u-s-officials-report-alleges-1401335072 Accessed: 1 March 2016.

[211] http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-woolen-goldfish-when-kittens-go-phishing Accessed: 1 March 2016.

[212] http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/TSPY_WOOLERG.A Accessed: 1 March 2016.

[213] http://www.washingtontimes.com/news/2009/apr/13/europe39s-telecoms-aid-with-spy-tech/print/ Accessed: 1 March 2016.

[214] http://www.reuters.com/article/us-iran-telecoms-idUSBRE82L0B820120322 Accessed: 1 March 2016.

[215] http://www.reuters.com/article/2012/04/10/us-zte-iran-aryacell-idUSBRE8390T720120410 Accessed: 1 March 2016.

Dec 2011	NetEnforcer, a product sold to Iran by an Israeli company ‘conducts "deep packet inspection’ of Internet networks, and has commercial uses such as optimizing traffic. Yet the software can also be used to intercept personal emails and other private data, or to prevent people from using the Web. According to the report, ‘deep packet inspection’ technology was previously used in Tunisia to arrest dissidents.”[216]
Sep 2012	“At the core of the Iranian network high-end equipment manufactured by the Chinese firm Huawei and capable of sophisticated online surveillance of traffic was discovered. The network is already ‘internally consistent and widely reachable,’ concluded the report [by University of Pennsylvania’s Center for Global Communications Studies], a copy of which was provided to The Washington Post.”[217]
Dec 2010	A joint statement by Mihanblog, Blogfa, and Cloob: “Notwithstanding the average blocking requests over recent years by the filtering authorities on particular blog cases, there has been a significant increase in blocking requests over the last few months. Such a trend will have dramatic effects on weakening the Persian blogosphere in general, and will have implications on discouraging Persian bloggers and negative consequences for Persian blogging services.”[218]
May 2015	Minister of Communications and Information Technology Mahmoud Vaezi met with Minister Lu Wei, Head of the Cyberspace Administration of the People’s Republic of China. The two discussed strengthening bilateral relations in various fields, specifically in cyberspace and information technology.[219]

[216] http://www.haaretz.com/israel-news/report-israeli-company-sold-surveillance-equipment-to-iran-1.403107 Accessed: 1 March 2016.

[217] https://www.washingtonpost.com/world/national-security/iran-preparing-internal-version-of-Internet/2012/09/19/79458194-01c3-11e2-b260-32f4a8db9b7e_story.html Accessed: 1 March 2016.

[218] http://admin.mihanblog.com/post/186 Accessed: 1 March 2016.

[219] http://goo.gl/Xjs1Wp Accessed: 1 March 2016.

Appendix 2: A brief overview of active hacking groups in Iran

- **Gerdab Group** (managed by the IRGC)[220]: Gerdab was mentioned at the beginning of this report. Details regarding their activities, a list of their operations[221], and a call for hiring hackers during the peak of the 2009 post-election disturbances[194] can be found in the links attached.
- **Shabgard Group:** Shabgard was one of the most famous hacking collectives in Iran. Though predating Ashiyane, Mohammad Jarjandi, the manager of the group, issued a farewell message on 5 March 2013 indicating the closure of the site. In this message he stated: “after three years of continuous and extreme oppression and due to the presence of an atmosphere of irrationally heavy security, we are closing Shabgard after 14 years of activity”.[223]
  A few months prior to publishing this statement, Jarjandi had published several articles criticising the authorities, including: “Corruption, the ruling axis of our present-day society,” “Free penetration tests for American and Israeli websites under the name of the followers of Velayat (followers of the Supreme Leader)”, “Legal sales of filter-breaking tools”, and “Making money from website blocking” which were most likely instrumental in the closure of his website by government authorities.[224]
- **Black Hat Group:** With 9,126 members and 600 site visitors per day,[224] Black Hat is mainly involved in the defacing of websites. Recently, they hacked one of the internal pages of Ashiyane’s website.[226]
- **Vampire Group:** This group set up a “Hacking Competition” in February 2015, in commemoration of the Islamic Revolution.
- **Iran Hack:** their website[227] describes the group as the following: “Iran Hack was formed in 2009 by a group of research students. The goal of this research group is to perform research and set up discussions and forums pertaining to the study and application of security software and coaxial systems. This group keeps up with the latest technological advances in the field. It has participated in numerous seminars and workshops and has received awards for its pioneering role in producing and studying security software. The group is made up of software developers, security researchers, and translators, and is producing content on a daily basis in order to elevate the knowledge of the general public with regards to network security.” The group has listed FATA Police, Gerdab group and the Ferdowsi University of Mashhad as their collaboration partners.
- **Hezbollah Cyber Army:** this group[228] has an extensive resume that includes hacking the ‘Majma Rohanioun Mobarez’ (a liberal clergy entity) and the ‘Baran Foundation’.[229] However, the HCA’s activity is not limited to hacking reformist websites.[230] In the ‘about’ section of the group’s website, they describe themselves in the following way: “Our message to the servants of the enemies is that HCA is God’s hand in taking revenge against the infidels. HCA has started an all-out Holy war that sees no borders. World powers and their servants can be sure that the officers of the HCA will always fight disbelief, oppression and polytheism. God willing, having the mobilized the forces of the oppressed and of the Islamic world on our side, we will not let the dictators, imperialists and their puppets rest. God willing.”[231]

[220] http://www.gerdab.ir/fa/content/3 Accessed: 1 March 2016.

[221] http://www.gerdab.ir/fa/list/18/16?service_id=18&cat_id=16&page=3 Accessed: 1 March 2016.

[222] http://goo.gl/iuJLd2 Accessed: 1 March 2016.

[223] https://web.archive.org/web/20140404205553/http://shabgard.org/ Accessed: 1 March 2016.

[224] https://web.archive.org/web/20140220171953/http://www.shabgard.org/ Accessed: 1 March 2016.

[225] http://black-hg.org/forums/ Accessed: 1 March 2016.

[226] http://www.zone-h.org/mirror/id/22596985 Accessed: 1 March 2016.

[227] http://iranhack.org/ Accessed: 1 March 2016.

[228] http://hcarmy.net/ Accessed: 1 March 2016.

[229] http://www.radiofarda.com/content/f12_two_khatami_related_sites_hacked/24497610.html Accessed: 1 March 2016.

[230] http://zone-h.org/archive/notifier=Hizbullah%20Cyber%20Army?zh=1 Accessed: 1 March 2016.

[231] http://hcarmy.net/about.html Accessed: 1 March 2016.

- **Iranian Dark Coder Team:** this group is currently working under the management of a hacker called MRSCO. Its forum has 3,439 members and a daily traffic of approximately 150 people. MRSCO operates another website for uploading shell codes.[232] Iranian Dark Coder Team has thus far defaced 4,319 websites.[234] The hacked websites include a subdomain of Microsoft,[235] Shahin Najafi (a singer-songwriter who is a critic of the Iranian regime),[207] and others deemed to be dissidents.[236] The team leader, who is also a member of the Ashiyane group, states: "On my gravestone, please write that this is the grave of a man who wanted to destroy Israel. Death to the murderer of Alireza's bright smiles, death to the bullet that wiped Armita's dreams, death to America."[237]

Appendix 3: A brief overview of the ownership of telephone and telecommunications assets in Iran

- **Telecommunication Company of Iran** (Hamrah Aval): 5% of the company shares belong to employees; 20% belong to 'Edaalat Stocks brokerage firms;' 50% +1 belong to 'Etemaad Mobin development Company;'[238] 20% belong to the government and the rest belong to other people or companies as shareholders.[239] Etemaad Mobin development Company is affiliated with the IRGC.[240]
- **Irancell:** South African MTN owns 49% of the shares and a consortium made up of Iranian Electronic Industry (SAIRAN) and 'The Foundation of the Oppressed and Veterans of Islamic Revolution' (or Bonyad for short), acting as 'The Iranian Electronics Development Company', have 51% of shares.[241] It is worth noting that SAIRAN is affiliated to the Iranian armed forces.
  Rightel: belongs to the SHASTA Corporation, which is affiliated with "The Social Security Organization" and Ministry of Social Welfare.[242]
- **Talia:** Mobin Iran Company and 'The Foundation of IRGC's Union' own The National Communication Company and 'Hamrah Aval', which is the largest telephone operator in the country. They are also owners of TALIA which is the largest telephone operator in the country and the first provider and operator of 'prepaid' SIM cards.[243]

[232] http://mrsco.mihanblog.com/post/45 Website: http://www.sh3ller.org Accessed: 1 March 2016.

[233] http://www.zone-h.org/archive/notifier=Iranian_Dark_Coders_Team Accessed: 1 March 2016.

[234] http://append-hc.com/mirror/id/115922 Accessed: 1 March 2016.

[235] http://www.zone-h.org/mirror/id/17598670 Accessed: 1 March 2016.

[236] http://ashiyane.org/forums/member.php?1059270-M-R-S-CO Accessed: 1 March 2016.

[237] http://idc-team.net/cc/showthread.php?t=656 Accessed: 1 March 2016.

[238] As of 13th December, this is no longer the case.

[239] http://www.tct.ir/?siteid=5&pageid=352&newsview=48251 Accessed: 1 March 2016.

[240] http://dw.com/p/Jq0n Accessed: 1 March 2016.

[241] http://www.telna.ir/News/3677/Default.aspx Accessed: 1 March 2016.

[242] http://www.citna.ir/nore/10766 Accessed: 1 March 2016.

[243] http://www.itna.ir/vdcdkf0x.yt0xo6a22y.html Accessed: 1 March 2016.

The following chart shows the number of users from each service provider:[244]

	Total No. Users	Prepaid	Postpaid	Active	3G/4G
Hamrah Aval	63,000,000	45,500,000	17,500,000	41,000,000	
Irancell	67,500,000	66,817,000		28,500,000	29,058,719
Rightel	5,000,000		134,000	1,300,000	
Talia	~1,000,000				

Appendix 4: Different modes of activity for the media and websites in the Soft War

Media Involvement in the Soft War

News Agency	Managing Director	In affiliation with	Political view
Tasnim	Majid Gholizadeh	IRGC	Conservative-hardliner
Fars	Seyed Nezam-aldin Musavi	IRGC	Conservative-hardliner
Al-Alam	Seyed Ahmad Sadat	IRIB	Conservative-centre
Mashregh News	Reza Davari		Conservative-hardliner
Bultan News	Babak Amini	IRGC	Conservative-hardliner
Enghelab News			
Shafaf News	Ehsan Rastegar	Mohammad Bagher Ghalibaf	
Shia News	Masud Bahraini	Strategic Institute for Global Discourse on Awaiting the Saviour	
Serat News	Ali Ghafurian		
Arsh News			
Farda News	Mohammad Saleh Meftah	Mohammad Bagher Ghalibaf	
Raja News	Meysam Nili Ahmadabadi		Conservative-hardliner
Press TV	Mohammad Akhgari		
Alef	Ahmad Tavakoli		
Fararu	Mohammad Hossein Khoshvaght		Conservative-centre
Pana	Mohammad Reza Khoshgoftar		
Rasa	Mohammad Mahdi Mohagheghi		
Shabestan	Arbab Soleimani	Mosque Affairs Centre	
Hemayat Online	Hesam-aldin Borumand	The Judiciary Promotion Centre	
Khabar Online	Alireza Moezzi	Ali Larijani	Conservative-centre
Young Journalists Club	Ali Mohammad Salehi	IRIB	Conservative-hardliner

[244] We have omitted the names of smaller companies such as SPADAN or Kishtel: http://www.ictna.ir/id/060127/ and http://goo.gl/3APxVN and http://goo.gl/cPCe4a Accessed: 1 March 2016.

Appendix 5: Bases of soft war officers' activities

Other than known and official media, there are many websites on which Soft War officers publish content. This appendix shows the most important bases of Soft War officers' activities. Most websites share a common approach toward the Soft War and even reproduce the same content.

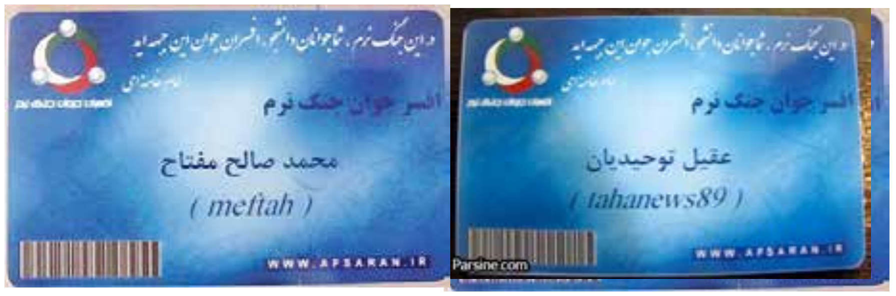
List of some websites active in the soft war[245]

Website	URL	Rating in Alexa	Rating in Iran
Tebyan	https://tebyan.net/	1729	31
Rasekhoon	http://rasekhoon.net/	4688	91
Aviny	http://www.aviny.com/	5581	119
Soft War Officers Club	http://www.afsaran.ir/	13340	292
Seraj Information System	http://seraj24.ir/	24432	373
Roshangari	http://roshangari.ir/	29136	556
Ammar Name	http://www.ammarname.ir/	38123	675
Ghasam	http://ghasam.ir/	50390	1076
Voice of Mostazafin	http://mostazafin.tv/	51483	1228
Iranian University Students News	http://iusnews.ir/	61315	1167
Basij Press	http://basijpress.ir/	76070	1345
Netiran Social Network	http://www.netiran.net/	92080	1761
Ghalam Children	http://bachehayeghalam.ir/	98974	1784
Book Room	http://bookroom.ir/	111547	1916
Didban	http://didban.ir/	121756	2218
Gerdab	http://www.gerdab.ir/	122679	2045
Mostazafin Tribunal	http://teribon.ir	140302	2341
Oweis - Muslim World Events	http://oweis.ir/	151867	3951
Ansar Clip - Voice of Truth and Vision	http://ansarclip.ir/	158762	3504
To Martyrs	http://www.tashohada.ir/	168706	3610
Soldiers of Islam	http://www.sarbazaneislam.com/	174126	3727
Mobin Media - Documentary and Speech Archive	http://mobinmedia.ir/	181287	3479
Hizbullah Cyber	http://hizbullahcyber.com/	234591	5940
Velayat - News agency of Supreme Leader Supporters	http://www.ehavadar.com/	756945	15942

[245] The ratings are taken from Alexa. They are not calculated based on the amount of soft war content each website published.

In addition to content provision, the websites employ strategies to attract and organise new members. Some websites, such as the Soft War Officers Club, issue ID cards for their members to make better use of the officers' capacities.[246]

Cyber Officer IDs



Appendix 6: Common methods of Internet filtering in Iran

Research on Iran's filtering methods is rare because of a lack of access to the country's internal networks and insufficient information being available in this regard on the Internet. Furthermore, informed people are afraid of participating in such studies. Iran also constantly changes its filtering techniques.[247] The following table provides some of them, to the best available knowledge of the researchers.

Type	date	Made by	Description
Proxy Servers IBB program manager [248]	2003	USA I Anonymizer, Inc.	Iranians can sometimes access 'forbidden' sites through proxy servers, although these machines can be blocked as well.
Content-Control software SmartFilter [249]	2006	San Jose firm Secure Computing	As of 2006, Iran's SmartFilter is configured to filter local Persian-language sites, and block prominent English-language sites, such as the websites for the *New York Times* and Facebook. The software effectively blocks access to most pornographic sites, gay and lesbian sites, reformist political sites, news media, sites that provide tools to help users cloak their Internet identity, and other sites nebulously defined as immoral on various grounds.

[246] http://www.donya-e-eqtesad.com/news/421261/ and http://www.afsaran.ir/link/16999 Accessed: 1 March 2016.

[247] https://jhalderm.com/pub/papers/iran-foci13.pdf Accessed: 1 March 2016.

[248] http://www.theregister.co.uk/2003/08/29/us_sponsors_anonymiser_if_you/ Accessed: 1 March 2016.

[249] https://opennet.net/sites/opennet.net/files/iranreport.pdf http://www.theguardian.com/technology/2006/dec/04/news.iran
https://www.newscientist.com/article/dn7589-iranian-net-censorship-powered-by-us-technology/
All accessed: 1 March 2016.

High-speed connections rate limitation [250]	2006		For nine years, the highest-speed Internet for household uses was 128 kbs, which prevented users from accessing multimedia content. The limitation was cancelled in June 2015.
Deep Packet Inspection [251]	2008	Nokia Siemens Systems (NSN)	TCI has a countrywide deep packet inspection capacity for monitoring or even altering content of Internet voice and mail communication and interception capability for 3G UMTS mobile networks.
ISP - Client Logs [252]	2009		Internet Service Providers (ISP) in Iran are required to store all the data sent or received by each of their clients. ISPs may delete the data no sooner than three months after the expiry of each client's contract.
Surveillance System capable of monitoring landline, mobile and Internet communications [253]	2010	Shenzhen, China-based ZTE Corp	The ZXMT system utilizes ‘deep packet inspection,’ a powerful and potentially intrusive technology that can read and analyse ‘packets’ of data that travel across the Internet. The technology can be used to track Internet users, search for and reconstruct email messages that have been broken up into data packets, block certain types of traffic, and even deliver altered web pages to users.
SSL-based traffic Limiting [253]	1 Jan 2011		ssl-based communications are being restricted to 2 kilobit per second rates or simply blocked altogether
Port Blocking [254]	1 Sep 2011		In the aftermath of the unrest in 2009, the regime began blocking all social websites, including Facebook, Youtube, Orkut, MySpace, and Twitter. The Iranians, however, started using VPN (virtual private network) connections to bypass censorship. Since Thursday 30 September 2011, all VPN ports have however been blocked, in the first attempt to start what the Iranian government calls the 'National Internet'.
Encrypted network traffic blocking [255]	1 Feb 2012		Iran started to filter SSL connections on much of their network
Tor blocking [256]	1 Sep 2012		Tor attempts to make its traffic look like a web browser communicating to an https web server, but closer examination can yield some differences.
The state-controlled telecommunications infrastructure [257]		Telecommunication Company of Iran	Iran has since developed its own hardware and software for filtering purposes. The architecture of the Iranian Internet is particularly conducive to widespread surveillance as all traffic from the dozens of ISPs serving households is routed through the state-controlled telecommunications infrastructure of the Telecommunication Company of Iran
Blue Coat Systems [258]		Planet Blue Coat Redux	Blue Coat Systems, a combination of network measurement and scanning methods and tools to identify instances of Blue Coat ProxySG and PacketShaper devices. This kind of equipment can be used to secure and maintain networks, but it can also be used to implement politically-motivated restrictions on access to information, and monitor and record private communications.
Refinement of HTTP hosts and keywords [259]			Sometimes, filtering is done through modifying HTTP host headers. In some other cases, access to specific keywords is blocked.
Disconnection and Internet rate limitation [260]			These disconnections either affect a single Internet protocol or apply to all Internet traffic. There have been reports on restrictions or blocking protocols such as HTTPS, VPN tunnels, and SSL.
DNS Injection [261]			The DNS filter does not only inject a spoofed response but also seems to drop the unwanted DNS query. Despite not sending any TCP packets, we received two TCP segments with an HTTP 403 error and FIN/ACK bits set and three TCP RST packets.

Other filtering methods observed include: IP Filtering, TCP Resetting, UDP Resetting and anti-filter blocking.

[250] http://www.tasnimnews.com/fa/news/1394/04/01/768026 Accessed: 1 March 2016.

[251] http://www.wsj.com/articles/SB124562668777335653 https://blog.networks.nokia.com/corporate-responsibility/2009/06/22/provision-of-lawful-intercept-capability-in-iran/ Accessed: 1 March 2016.

[252] http://www.presstv.com/detail.aspx?id=101138&sectionid=351020101
http://www.wsj.com/articles/SB125978649644673331 All accessed: 1 March 2016.

[253] http://www.reuters.com/article/2012/03/22/us-iran-telecoms-idUSBRE82L0B820120322 Accessed: 1 March 2016.

[254] https://blog.torproject.org/blog/new-blocking-activity-iran Accessed: 1 March 2016.

[255] http://www.reuters.com/article/2013/03/10/us-iran-Internet-idUSBRE9290CV20130310 Accessed: 1 March 2016.

[256] http://www.ibtimes.com/cyber-rebels-see-way-get-around-irans-vpn-Internet-block-1118671 Accessed: 1 March 2016.

[257] https://blog.torproject.org/blog/iran-blocks-tor-tor-releases-same-day-fix Accessed: 1 March 2016.

[258] http://opennet.net/research/profiles/iran Accessed: 1 March 2016.

[259] https://citizenlab.org/2013/07/planet-blue-coat-redux/ Accessed: 1 March 2016.

[260] https://www.usenix.org/conference/foci13/workshop-program/presentation/aryan Accessed: 1 March 2016.

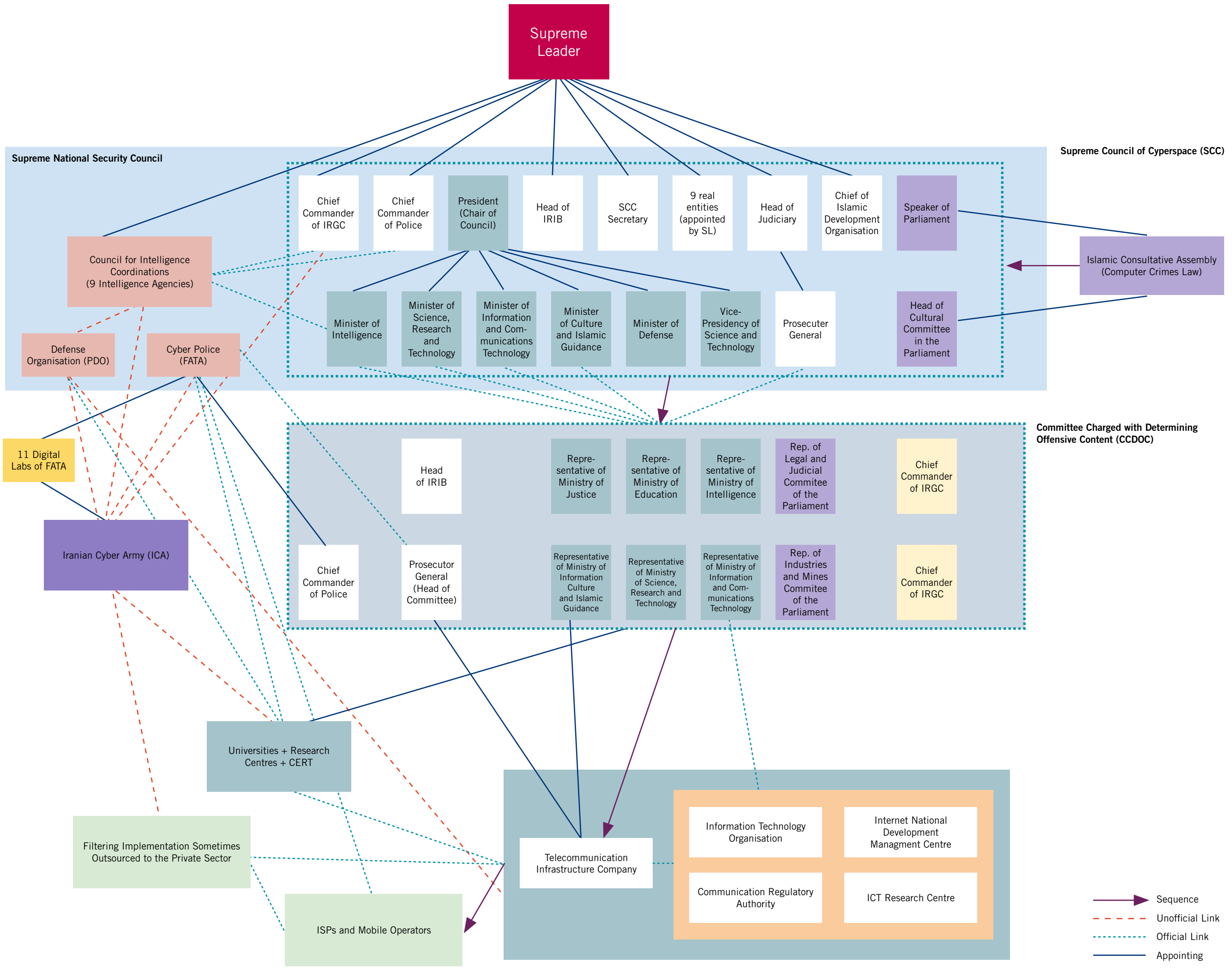
[261] http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6814824 Accessed: 1 March 2016.

Appendix 7: Sharif University Exclusive Programme on “Security and Counter-infiltration”

Programme includes:

1. Introduction to networks and Linux coding
2. Identification and Footprinting
3. Operating systems analysis and scanning
4. Enumeration
5. Access Entry
6. Metasploit, Kali, and Backtrack introduction to operating systems
7. Escalating privilege
8. Creating backdoors
9. Infiltration/breach tests for personal computers
10. Service denial or DoS Attacks
11. Infiltration/breach tests for websites
12. Infiltration/breach tests for databases
13. Infiltration/breach tests internal networks
14. Infiltration/breach tests for routers
15. Infiltration/breach tests for wireless networks
16. Rootkit installation and identification
17. Covering tracks
18. Infiltrating IDS – Firewall systems
19. Cryptography
20. Email security and introduction to infiltration/breach tests
21. SQL Injection
22. Identifying security loopholes for command execution
23. Identifying security loopholes for file inclusion in web based software/applications
24. Identifying security loopholes for XSS in web based software/applications
25. Exploit writing in PHP and Perl

Appendix 8: The mechanism and authorities involved in filtering and censorship


Supreme Leader
Supreme National Security Council
Supreme Council of Cyperspace (SCC)
Chief Commander of IRGC
Chief Commander of Police
President (Chair of Council)
Head of IRIB
SCC Secretary
9 real entities (appointed by SL)
Head of Judiciary
Chief of Islamic Development Organisation
Speaker of Parliament
Council for Intelligence Coordinations (9 Intelligence Agencies)
Islamic Consultative Assembly (Computer Crimes Law)
Minister of Intelligence
Minister of Science, Research and Technology
Minister of Information and Com-munications Technology
Minister of Culture and Islamic Guidance
Minister of Defense
Vice-Presidency of Science and Technology
Prosecuter General
Head of Cultural Committee in the Parliament
Defense Organisation (PDO)
Cyber Police (FATA)
11 Digital Labs of FATA
Committee Charged with Determining Offensive Content (CCDOC)
Head of IRIB
Repre-sentative of Ministry of Justice
Repre-sentative of Ministry of Education
Repre-sentative of Ministry of Intelligence
Rep. of Legal and Judicial Commitee of the Parliament
Chief Commander of IRGC
Iranian Cyber Army (ICA)
Chief Commander of Police
Prosecutor General (Head of Committee)
Representative of Ministry of Information Culture and Islamic Guidance
Representative of Ministry of Science, Research and Technology
Representative of Ministry of Information and Com-munications Technology
Rep. of Industries and Mines Commitee of the Parliament
Chief Commander of IRGC
Universities + Research Centres + CERT
Filtering Implementation Sometimes Outsourced to the Private Sector
ISPs and Mobile Operators
Telecommunication Infrastructure Company
Information Technology Organisation
Internet National Development Managment Centre
Communication Regulatory Authority
ICT Research Centre
Sequence
Unofficial Link
Official Link
Appointing

DEFENDING FREEDOM
OF EXPRESSION AND INFORMATION

ARTICLE 19 Free Word Centre 60 Farringdon Road London EC1R 3GA
T +44 20 7324 2500 F +44 20 7490 0566
E info@article19.org W www.article19.org Tw @article19org facebook.com/article19org